(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年6 月23 日 (23.06.2005)

PCT

(10) 国際公開番号
WO 2005/057447 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP2004/017758

(22) 国際出願日: 2004 年11 月30 日 (30.11.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-410784 2003 年12 月9 日 (09.12.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 野仲 真佐男 (NONAKA, Masao). 館林 誠 (TATEBAYASHI, Makoto). 大森 基司 (OHMORI, Motoji).

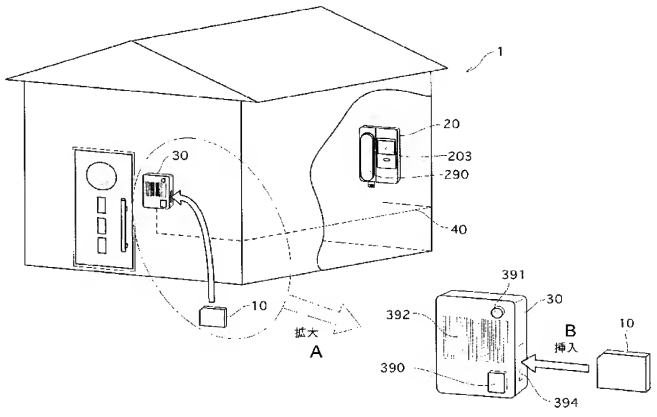
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: AUTHENTICATION SYSTEM, AUTHENTICATION DEVICE, AND RECORDING MEDIUM

(54) 発明の名称: 認証システム、認証装置及び記録媒体



A... ENLARGED
B... INSERT

(57) Abstract: There is provided an authentication system for authenticating various validities of a visit of a home delivery service man. The authentication system includes an authentication card, a user terminal, and a card reader. When the authentication card is inserted into the card reader, the user terminal generates a random number, stores the random number generated, and outputs it to the authentication card. The authentication card encrypts the received random number by an identification key stored in advance, generates encrypted information, and outputs the encrypted information generated to the user terminal. The user terminal decrypts the received encrypted information by using the authentication key stored in advance, generates the decryption result, and judges whether the generated decryption result coincides with the random number stored, thereby performing authentication.

(57) 要約: 宅配業者による訪問の各種の正当性を認証する認証システムを提供する。 身元認証システムは、認証カードと、ユーザ端末と、カードリーダとから構成される。ユーザ端末は、カードリーダに認証カードが挿入されると、乱数を生成し、生成した乱数を記憶するとともに、認証カードへ出力する。認証カードは、予め記憶している身元証明鍵にて受け取った乱数を暗号化して、暗号化情報を生成し、生成した暗号化情報をユーザ端末へ出力する。ユーザ端末は、受け取った暗号化情報を予め記憶している身元認証鍵を用いて復号し

[続葉有]

WO 2005/057447 A1

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

て、復号結果を生成し、生成した復号結果と記憶している乱数とが一致するか否か判断することによる認証を行う。

明 細 書

認証システム、認証装置及び記録媒体

技術分野

[0001] 本発明は、記録媒体の所有者の身元を認証する技術に関する。

背景技術

[0002] 従来、宅内にいる者が、訪問者の身元をインターホンやテレビドアホンなどを利用して確認する方法が一般的に用いられている。

しかしながら、上記の方法では、訪問者が容姿や声を偽ることによって、宅内にいる者を欺くことができるため、宅内にいる者が、訪問者の身元を確実に確認することは困難である。

[0003] そこで、以下に示すような個人情報表示システムが開示されている。この個人情報表示システムは、個人情報及び個人特定情報を予め記憶しているサーバと、個人特定情報を入力する入力装置と、個人特定情報を通信回線を介してサーバに送信するユーザ端末とを有している。

入力装置は、指紋入力装置を有しており、指紋入力装置より、訪問者の指紋を受け付け、受け付けた指紋から生成される指紋情報を、個人特定情報としてユーザ端末へ出力する。ユーザ端末は、個人特定情報を受け取り、受け取った個人特定情報をサーバへ送信する。サーバは、予め記憶している個人特定情報とユーザ端末から送信された個人特定情報とを照合し、照合結果に応じて、個人特定情報と関連付けられて記憶している個人情報をユーザ端末に送信する。ユーザ端末は、サーバから受信した個人情報を表示する。

[0004] この個人情報表示システムによって、宅配業者等の訪問者の身分を確実に確認することが可能、つまり訪問者による訪問の正当性を確認することが可能になる。

発明の開示

発明が解決しようとする課題

[0005] しかしながら、上記に示す個人情報表示システムは、訪問者の指紋情報により、訪問者個人の正当性を認証することはできるが、宅配業者といった団体の正当性、訪

問内容の正当性のような他の種の正当性の認証を行うことはできない。

そこで、本発明は、従来技術では行えなかった、宅配業者による訪問の各種の正当性を認証する認証システム、認証装置、記録媒体、認証方法、認証プログラム及びプログラム記録媒体を提供することを目的とする。

課題を解決するための手段

[0006] 上記目的を達成するために、本発明は、宅配業者が有する可搬型の記録媒体と、前記宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者による訪問の正当性を認証する認証装置と、前記記録媒体と前記認証装置との間における情報の入出力を行い、玄関先に設けられた入出力装置とからなる認証システムであって、前記記録媒体は、前記宅配業者による訪問の正当性に係る情報を、少なくとも1つ予め記憶しており、前記認証装置は、前記宅配業者による訪問の正当性の検証に係る情報を、少なくとも1つ記憶しており、前記入出力装置を介して、前記記録媒体に記憶されている前記情報と、当該装置にて記憶している前記情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断することを特徴とする。

発明の効果

[0007] 上記に示した構成によると、認証システムの認証装置は、入出力装置を介して、宅配業者が有する記録媒体の記憶されている情報と、前記宅配業者による訪問の正当性の検証に係る情報とを用いた認証を行い、訪問業者による訪問の正当性を判断することができる。従来の個人情報表示システムでは、訪問者その者の正当性のみ認証することができたが、本発明では、記録媒体に、宅配業者による訪問の正当性に係る情報を記憶することにより、認証装置は、訪問者の正当性の認証とは、異なる各種の正当性の認証を行うことができる。また、訪問を受ける者は、家屋内に居ながらにして、訪問業者による訪問は正当であるか否かを知ることができる。

[0008] ここで、前記記録媒体は、ICカードであり、前記入出力装置は、前記ICカードのカードリーダであり、前記カードリーダは、さらに、玄関ドアの施錠状態を検出し、前記認証装置は、前記カードリーダにて玄関ドアが施錠されている状態が検出された場合に、前記認証を行うとしてもよい。

この構成によると、認証システムの認証装置は、玄関ドアを施錠した状態で認証を行うことができる。これにより、訪問を受ける者は、認証装置による認証処理が終了するまで、訪問者を家屋内に招き入れることなく、認証結果に応じて、訪問者を招き入れるか否かを判断することができる。つまり、認証装置が、訪問業者による訪問が正当であると判断する場合には、訪問を受ける者は、玄関ドアの施錠を解除して、訪問者を招き入れることができる。

[0009] ここで、前記ICカードは、前記宅配業者による訪問の正当性に係る情報として、前記宅配業者の正当性を証明する証明情報を記憶しており、前記認証装置は、前記宅配業者による訪問の正当性の検証に係る情報として、前記証明情報を検証するための認証情報を記憶しており、前記認証装置は、前記証明情報と記憶している前記認証情報とを用いて、前記カードリーダを介して、前記宅配業者による訪問が正当であるか否かの認証を行うとしてもよい。

[0010] この構成によると、認証システムの認証装置は、ICカードに記憶されている証明情報と、当該認証装置が記憶している認証情報とを用いた認証を行うことができる。

ここで、前記ICカードは、前記宅配業者による訪問の正当性に係る情報として、さらに、前記宅配業者による訪問の内容を示す第1訪問情報を予め記憶しており、前記認証装置は、前記宅配業者による訪問の正当性の検証に係る情報として、さらに、前記第1訪問情報にて示される情報を検証するための第2訪問情報を記憶しており、前記認証装置は、前記証明情報と前記認証情報とを用いた認証の結果が肯定的である場合に、前記ICカードより前記カードリーダを介して、前記第1訪問情報を取得し、取得した前記第1訪問情報と、記憶している前記第2訪問情報とが一致するか否かを判断し、判断結果が肯定的である場合に、前記宅配業者による訪問が正当であると判断するとしてもよい。

[0011] この構成によると、認証システムの認証装置は、証明情報と、認証情報とを用いた認証の結果が肯定的であり、第1訪問情報と、第2訪問情報とが一致する場合に、訪問業者による訪問が正当であると判断することができる。つまり、認証装置は、訪問業者が正当な訪問業者であり、且つその訪問業者の訪問内容が正当なものである場合に、訪問業者による訪問が正当であると判断する。これにより、訪問を受ける者は、

正当な訪問業者による不正な訪問を避けることができる。例えば、正当な訪問業者であると偽った不正な訪問を避けることができる。

[0012] ここで、前記第1訪問情報は、宅配業者による訪問の時間帯を示す第1時間情報であり、前記第2訪問情報は、宅配業者にて訪問を受ける時間帯を示す第2時間情報であり、前記認証装置は、前記第1時間情報と前記第2時間情報とが一致するか否かを判断するとしてもよい。

この構成によると、認証システムは、第1訪問情報を、訪問業者が訪問する時間帯とし、第2訪問情報を、訪問を受ける時間帯とし、認証装置は、それぞれにて示される時間帯が一致する場合に、訪問業者による訪問が正当であると判断することができる。

[0013] ここで、前記第1訪問情報は、宅配業者の訪問内容を示す第1訪問内容情報であり、前記第2訪問情報は、宅配業者にて訪問を受ける内容を示す第2訪問内容情報であり、前記認証装置は、前記第1訪問内容情報と前記第2訪問内容情報とが一致するか否かを判断するとしてもよい。

この構成によると、認証システムは、第1訪問情報を、訪問業者による訪問業者による訪問内容とし、第2訪問情報を、訪問を受ける訪問内容とし、認証装置は、それぞれにて示される訪問内容が一致する場合に、訪問業者による訪問が正当であると判断することができる。

[0014] ここで、前記第1訪問情報は、宅配業者による訪問の時間帯を示す第1時間情報と、宅配業者の訪問内容を示す第1訪問内容情報とを含み、前記第2訪問情報は、宅配業者にて訪問を受ける時間帯を示す第2時間情報と、宅配業者にて訪問を受ける内容を示す第2訪問内容情報とを含み、前記認証装置は、前記第1時間情報と前記第2時間情報とが一致するか否か、及び前記第1訪問内容情報と前記第2訪問内容情報とが一致するか否かを判断するとしてもよい。

[0015] この構成によると、認証システムは、第1訪問情報を、訪問業者による訪問業者による訪問の時間帯と訪問内容とし、第2訪問情報を、訪問を受ける時間帯と訪問内容とし、認証装置は、それぞれにて示される時間帯及び訪問内容が一致する場合に、訪問業者による訪問が正当であると判断することができる。

ここで、前記ICカードは、さらに、前記宅配業者にて届けられた物品に係る物品情報を記憶しており、前記認証装置は、さらに、前記ICカードより前記カードリーダを介して、前記物品情報を取得し、前記宅配業者による訪問が正当であると判断する場合に、前記物品情報を表示するとしてもよい。

[0016] この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、ICカードより取得した物品情報を表示することができる。

ここで、前記物品情報は、送り主の名前であり、前記認証装置は、前記ICカードより送り主の名前を取得し、取得した名前を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、物品の送り主の名前を表示することができる。これにより、訪問を受ける者は、物品の送り主を知ることにより、送り主が見ず知らずの人の名前である場合には、物品の受け取りを拒否することができるようになり、不審な送り主から送られた物品の受け取りを拒否することができる。

[0017] ここで、前記物品情報は、前記物品の物品名であり、前記認証装置は、前記ICカードより前記物品の物品名を取得し、取得した物品名を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、物品の物品名を表示することができる。これにより、訪問を受ける者は、物品名を知ることにより、不審な物品の受け取りを拒否することができるようになる。

[0018] ここで、前記物品情報は、送り主からのメッセージであり、前記認証装置は、前記ICカードより送り主からのメッセージを取得し、取得したメッセージを表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、物品の送り主からのメッセージを表示することができる。

[0019] ここで、前記ICカードは、訪問者を識別する訪問者情報を記憶しており、前記認証装置は、さらに、前記ICカードより前記カードリーダを介して、前記訪問者情報を取得し、前記宅配業者による訪問が正当であると判断する場合に、前記訪問者情報を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、ICカードより取得した訪問者情報を表示することができる。

[0020] ここで、前記訪問者情報は、訪問者の名前であり、前記認証装置は、前記ICカードより訪問者の名前を取得し、取得した名前を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、訪問者の名前を表示することができる。訪問を受ける者は、玄関ドアのドア穴越しに、訪問者が付けている名札に記載されている名前と表示された名前とが一致するか否かを確認することができる。

[0021] ここで、前記訪問者情報は、訪問者の顔写真の画像であり、前記認証装置は、前記ICカードより前記訪問者の顔写真の画像を取得し、取得した顔写真の画像を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、訪問者の顔写真の画像を表示することができる。訪問を受ける者は、玄関ドアのドア穴越しに、訪問者の顔と、表示された顔写真の画像とが一致するか否かを確認することができる。

[0022] ここで、前記訪問者情報は、訪問者の名前、及び顔写真の画像であり、前記認証装置は、前記ICカードより前記訪問者の名前、及び顔写真の画像を取得し、取得した名前、及び顔写真の画像を表示するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問が正当であると判断する場合に、訪問者の名前及び顔写真の画像を表示することができる。訪問を受ける者は、玄関ドアのドア穴越しに、訪問者が付けている名札に記載されている名前と表示された名前とが一致するか否かを確認、及び訪問者の顔と、表示された顔写真の画像とが一致するか否かを確認することができる。

[0023] ここで、前記認証装置及び前記ICカードは、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行うとしてもよい。

この構成によると、認証システムの認証装置は、証明情報と認証情報とを用いたチャレンジレスポンス型による認証を行うことができる。

ここで、前記証明情報は、暗号化鍵であり、前記認証情報は、復号鍵であり、前記

認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記暗号化鍵を用いて暗号化して、レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記復号データを用いて前記レスポンスを復号して、復号データを生成して、生成した復号データと、前記チャレンジデータとが一致するか否かの認証を行うとしてもよい。

[0024] この構成によると、認証システムの認証装置は、ICカードにて記憶されている暗号化鍵を用いて、チャレンジデータが暗号化されたレスポンスデータを、ICカードより受け取り、受け取ったレスポンスデータを復号し、その復号結果と、チャレンジデータとを用いて、認証を行うことができる。これにより、認証装置とICカードとの間の伝送路において、盗聴がされた場合、伝送路にて流れる情報は、暗号化されているためセキュリティが確保される。また、盗聴されたレスポンスデータが復号された場合においても、チャレンジデータが暴露されるだけであり、訪問業者の正当性を示す証明情報は、暴露されないという効果もある。

[0025] ここで、前記暗号化鍵は、前記ICカードの所有者の生体科学的特徴を示す所有者証明情報であり、前記認証装置は、さらに、訪問者の生体科学的特徴を示す所有者認証情報を受け付け、受け付けた所有者認証情報を、前記復号鍵とするとしてもよい。

この構成によると、認証システムは、暗号化鍵を、ICカードの所有者の生体科学的特徴を示す所有者証明情報とし、復号鍵を訪問者の生体科学的特徴を示す所有者認証情報とすることができる。

[0026] ここで、前記認証装置は、さらに、前記復号鍵を配信する配信装置とネットワークを介して接続されており、前記認証装置は、さらに、前記宅配業者の訪問を受ける前に、前記配信装置から配信される前記復号鍵を受信し、受信した前記復号鍵を記憶するとしてもよい。

この構成によると、認証システムの認証装置は、訪問業者による訪問前に、配信装

置から復号鍵を受信し、記憶することができる。

[0027] ここで、前記認証情報は、秘密鍵であり、前記ICカードは、前記秘密鍵と同一の鍵に対して、一方向性関数が施された第1鍵を記憶しており、前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記第1鍵を用いて暗号化して、レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記秘密鍵に、前記前記一方向性関数と同一の処理を行う関数を施して第2鍵を生成し、生成した前記第2鍵を用いて、前記レスポンスを復号して、復号データを生成して、生成した復号データと、前記チャレンジデータとが一致するか否かの認証を行うとしてもよい。

[0028] この構成によると、認証システムの認証装置は、ICカードにて記憶されている第1鍵を用いて、チャレンジデータが暗号化されたレスポンスデータを、ICカードより受け取り、第2鍵を生成して、生成した第2鍵を用いて、受け取ったレスポンスデータを復号し、その復号結果と、チャレンジデータとを用いて、認証を行うことができる。これにより、認証装置とICカードとの間の伝送路において、盗聴がされた場合、伝送路にて流れる情報は、暗号化されているためセキュリティが確保される。また、盗聴されたレスポンスデータが復号された場合においても、チャレンジデータが暴露されるだけであり、訪問業者の正当性を示す証明情報は、暴露されないという効果もある。また、ICカード内に記憶している第1鍵が暴露された場合、一方向性関数の性質より、第1鍵から秘密鍵を生成することは不可能であるため、秘密鍵は暴露されないという効果もある。

[0029] ここで、前記認証情報は、第1秘密鍵であり、前記ICカードは、前記第1秘密鍵と同一の内容である第2秘密鍵を記憶しており、前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記第2秘密鍵を用いて暗号化して、レスポンスデータを

生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記第1秘密鍵を用いて前記チャレンジデータを暗号化して、暗号化データを生成し、生成した前記暗号化データと、前記レスポンスデータとが一致するか否かの認証を行うとしてもよい。

[0030] この構成によると、認証システムの認証装置は、ICカードにて記憶されている第1鍵を用いて、チャレンジデータが暗号化されたレスポンスデータを、ICカードより受け取り、暗号化データを生成して、生成した暗号化データとレスポンスデータを用いて、認証を行うことができる。

ここで、前記証明情報は、秘密鍵であり、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、前記秘密鍵を用いて、受け取った前記チャレンジデータの電子署名を生成し、生成した電子署名を前記レスポンスデータとして、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記公開鍵と前記チャレンジデータとを用いて、前記チャレンジデータの署名検証による認証を行うとしてもよい。

[0031] この構成によると、認証システムの認証装置は、電子署名を用いたチャレンジレスポンス型の認証を行うことができる。

ここで、前記秘密鍵は、前記ICカードの所有者の生体科学的特徴を示す所有者証明情報であり、前記認証装置は、さらに、訪問者の生体科学的特徴を示す所有者認証情報を受け付け、受け付けた所有者認証情報を、前記公開鍵とするとしてもよい。

[0032] この構成によると、認証システムは、電子署名に用いる秘密鍵を、ICカードの所有者の生体科学的特徴を示す所有者証明情報とし、署名の検証に用いる公開鍵を訪問者の生体科学的特徴を示す所有者認証情報とすることができる。

ここで、前記証明情報は、秘密鍵であり、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記公開鍵を用いて暗号化し、前記暗号化されたチャレンジデータを、前記

カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記認証装置より前記暗号化されたチャレンジデータを受け取り、前記秘密鍵を用いて、受け取った前記暗号化されたチャレンジデータを復号して、前記レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、受け取った前記レスポンスデータと、前記チャレンジデータとが一致するか否かの認証を行うとしてもよい。

[0033] この構成によると、認証システムの認証装置は、公開鍵を用いてチャレンジデータを暗号化し、ICカードは、暗号化されたチャレンジデータを復号してレスポンスデータを生成して、認証装置へ出力し、認証装置は、チャレンジデータとレスポンスデータを用いて、認証を行うことができる。

ここで、前記ICカードは、前記公開鍵を含み、且つ前記公開鍵の正当性を証明する公開鍵証明書を記憶しており、前記認証装置は、さらに、前記公開鍵証明書を、前記ICカードから取得し、取得した前記公開鍵証明書の正当性を検証し、検証結果が肯定的である場合に、前記公開鍵証明書に含まれる前記公開鍵を、記憶するとしてもよい。

[0034] この構成によると、認証システムの認証装置は、ICカードにて記憶している公開鍵証明書から公開鍵を取得し、記憶することができる。

ここで、前記ICカードは、宅配業者が訪問前に前記認証装置へに配布した第1訪問鍵と同一の第2訪問鍵を記憶しており、前記認証装置は、さらに、前記第1訪問鍵を記憶しており、前記認証装置は、チャレンジレスポンスによる認証の結果が肯定的である場合に、さらに、第1訪問検証データを生成し、生成した前記訪問検証データを、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記訪問検証データを受け取ると、前記第2訪問鍵を用いて、受け取った前記訪問検証データを暗号化し、前記暗号化された訪問検証データを、前記カードリーダを介して前記認証装置へ出力し、前記認証装置は、前記第1訪問鍵を用いて、受け取った暗号化された訪問検証データを復号して、復号結果と、前記訪問検証データとが一致するか否かを判断し、一致する場合に、第1訪問情報と第2訪問情報とが一致するか否かを

判断するとしてもよい。

[0035] この構成によると、認証システムの認証装置は、証明情報と認証情報とを用いたチャレンジレスポンス型による認証の結果が肯定的である場合に、第1訪問鍵及び第2訪問鍵とを用いた認証を行うことができる。

ここで、前記認証装置は、前記ICカードへ前記チャレンジデータを出力する際に、前記チャレンジデータのデータ構造とは異なるデータ構造からなり、且つ前記チャレンジデータと同一の内容を示す変換チャレンジ情報へと変換し、前記変換チャレンジ情報を前記チャレンジデータとして前記ICカードへ出力するとしてもよい。

[0036] この構成によると、認証システムの認証装置は、チャレンジデータを、ICカードへ出力する際に、チャレンジデータを用いて、変換チャレンジ情報を生成し、生成した変換チャレンジ情報を、チャレンジデータとしてICカードへ出力することができる。

ここで、前記ICカードは、前記認証装置へ前記レスポンスデータを出力する際に、前記レスポンスデータのデータ構造とは異なるデータ構造からなり、且つ前記レスポンスデータと同一の内容を示す変換レスポンス情報へと変換し、前記変換レスポンス情報を前記レスポンスデータとして前記認証装置へ出力するとしてもよい。

[0037] この構成によると、認証システムのICカードは、レスポンスデータを、認証装置へ出力する際に、レスポンスデータを用いて、変換レスポンス情報を生成し、生成した変換レスポンス情報を、レスポンスデータとして認証装置へ出力することができる。

ここで、前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなり、前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなるとしてもよい。

[0038] この構成によると、認証システムの認証装置は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換チャレンジ情報を、ICカードへ出力し、ICカードは、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換レスポンス情報を、認証装置へ出力することができる。

ここで、前記認証装置は、さらに、自己を識別する装置識別子を記憶しており、前記認証装置は、前記宅配業者による訪問が正当であると判断する場合に、前記装置識別子を、前記カードリーダを介して前記ICカードへ出力し、前記ICカードは、前記

認証装置から前記装置識別子を受け取ると、受け取った前記装置識別子を記憶するとしてもよい。

[0039] この構成によると、認証システムの認証装置は、装置識別子をICカードへ出力することができる。

また、本発明は、宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者が有する可搬型の記録媒体を用いて、前記宅配業者の訪問の正当性を認証する認証装置であって、前記認証の処理に用いる情報を記憶している情報記憶手段と、玄関先に設けられた入出力装置を介して、前記記録媒体が記憶している前記訪問業者による訪問の正当性に係る情報と、前記情報記憶手段にて記憶している情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する判断手段とを備えることを特徴とする。

[0040] この構成によると、認証装置は、入出力装置を介して、宅配業者が有する記録媒体の記憶されている情報と、当該装置が記憶している情報とを用いた認証を行い、訪問業者による訪問の正当性を判断することができる。従来の個人情報表示システムでは、訪問者の正当性のみ認証することができたが、本発明では、記録媒体に、宅配業者による訪問の正当性に係る情報を記憶することにより、認証装置は、訪問者の正当性の認証とは、異なる種の正当性の認証を行うことができる。また、訪問を受ける者は、家屋内に居ながらにして、訪問業者による訪問は正当であるか否かを知ることができる。

[0041] ここで、前記入出力装置は、前記記録媒体のカードリーダであり、前記カードリーダは、玄関ドアの施錠状態を検出し、前記判断手段は、前記カードリーダにて玄関ドアが施錠されている状態が検出された場合に、前記認証を行うとしてもよい。

この構成によると、認証装置は、玄関ドアを施錠した状態で認証を行うことができる。これにより、訪問を受ける者は、認証装置による認証処理が終了するまで、訪問者を家屋内に招き入れることなく、認証結果に応じて、訪問者を招き入れるか否かを判断することができる。つまり、認証装置が、訪問業者による訪問が正当であると判断する場合には、訪問を受ける者は、玄関ドアの施錠を解除して、訪問者を招き入れることができる。

[0042] ここで、前記記録媒体は、前記宅配業者による訪問の正当性に係る情報として、前記宅配業者の正当性を証明する証明情報を記憶しており、前記情報記憶手段は、前記認証の処理に用いる情報として、前記宅配業者の正当性を検証する認証情報を記憶しており、前記判断手段は、前記証明情報と記憶している前記認証情報とを用いて、前記カードリーダを介して、前記宅配業者による訪問が正当であるか否かの認証を行うとしてもよい。

[0043] この構成によると、認証装置は、認証情報と証明情報とを用いた認証を行うことができる。

ここで、前記記録媒体は、前記宅配業者による訪問の正当性に係る情報として、さらに、前記宅配業者による訪問の内容を示す第1訪問情報を予め記憶しており、前記情報記憶手段は、さらに、前記第1訪問情報にて示される情報を検証するための第2訪問情報を記憶しており、前記判断手段は、前記証明情報と前記認証情報とを用いた認証の結果が肯定的である場合に、前記記録媒体より前記カードリーダを介して、前記第1訪問情報を取得し、取得した前記第1訪問情報と、記憶している前記第2訪問情報とが一致するか否かを判断し、判断結果が肯定的である場合に、前記宅配業者による訪問が正当であると判断するとしてもよい。

[0044] この構成によると、認証装置は、証明情報と、認証情報とを用いた認証の結果が肯定的であり、第1訪問情報と、第2訪問情報とが一致する場合に、訪問業者による訪問が正当であると判断することができる。つまり、認証装置は、訪問業者が正当な訪問業者であり、且つその訪問業者の訪問内容が正当なものである場合に、訪問業者による訪問が正当であると判断する。これにより、訪問を受ける者は、正当な訪問業者による不正な訪問を避けることができる。例えば、正当な訪問業者であると偽った不正な訪問を避けることができる。

[0045] ここで、前記記録媒体は、さらに、前記宅配業者にて届けられた物品に係る物品情報を記憶しており、前記認証装置は、さらに、前記記録媒体より前記カードリーダを介して、前記物品情報を取得する物品情報取得手段と、前記判断手段による判断の結果が肯定的である場合に、前記物品情報を表示する物品情報表示手段とを備えるとしてもよい。

この構成によると、認証装置は、訪問業者による訪問が正当であると判断する場合に、記録媒体より取得した物品情報を表示することができる。

[0046] ここで、前記記録媒体は、訪問者を識別する訪問者情報を記憶しており、前記認証装置は、さらに、前記記録媒体より前記カードリーダを介して、前記訪問者情報を取得する訪問者情報取得手段と、前記判断手段による判断の結果が肯定的である場合に、前記訪問者情報を表示する訪問者情報表示手段とを備えるとしてもよい。

この構成によると、認証装置は、訪問業者による訪問が正当であると判断する場合に、記録媒体より取得した訪問者情報を表示することができる。

[0047] ここで、前記認証装置及び前記記録媒体は、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行うとしてもよい。

この構成によると、認証装置は、証明情報と認証情報とを用いたチャレンジレスポンス型による認証を行うことができる。

ここで、前記認証装置は、携帯電話機であるとしてもよい。

[0048] この構成によると、認証装置は、携帯電話機とすることができる。

また、本発明は、宅配業者が有し、前記宅配業者の訪問を受ける者の家屋内に設けられ、前記宅配業者による正当性を認証する認証装置に用いられる可搬型の記録媒体であって、前記宅配業者による訪問の正当性に係る情報を、少なくとも1つ予め記憶している記憶手段と、前記認証装置から玄関先に設けられた入出力装置を介して、第1データを受け取る受取手段と、前記記憶手段にて記憶している情報を用いて、認証の処理に用いられる第2データを、前記第1データより生成するデータ生成手段と、生成した前記第2データを、前記入出力装置を介して前記認証装置へ出力する出力手段とを備えることを特徴とする。

[0049] この構成によると、記録媒体は、認証装置から入出力装置を介して、第1データを受け取り、記憶している情報を用いて、認証の処理に用いられる第2データを、受け取った第1データより生成し、生成した第2データを認証装置へ出力することができる。これにより、認証装置は、訪問者を家屋の外にある記録媒体から、認証の処理に必要な第2データを取得することができる。

[0050] ここで、前記記憶手段は、前記宅配業者による訪問の正当性に係る情報として、前

記宅配業者の正当性を証明する証明情報を記憶しており、前記データ生成手段は、前記証明情報を用いて、前記第2データを生成するとしてもよい。

この構成によると、記録媒体は、証明情報を用いて、第2データを生成することができる。

[0051] ここで、前記記憶手段は、前記宅配業者による訪問の正当性に係る情報として、さらに、前記宅配業者による訪問の内容を示す訪問情報を予め記憶しており、前記出力手段は、さらに、前記訪問情報を、前記入出力装置を介して前記認証装置へ出力するとしてもよい。

この構成によると、記録媒体は、宅配業者による訪問の正当性の係る情報として訪問情報を記憶し、記憶している訪問情報を認証装置へ出力することができる。

[0052] ここで、前記記録媒体は、さらに、前記宅配業者にて届けられた物品に係る物品情報を記憶している物品情報記憶手段を備え、前記出力手段は、さらに、前記物品情報を、前記入出力装置を介して前記認証装置へ出力するとしてもよい。

この構成によると、記録媒体は、物品に係る物品情報を記憶し、記憶している物品情報を認証装置へ出力することができる。

[0053] ここで、前記記録媒体は、さらに、訪問者を識別する訪問者情報を記憶している訪問者情報記憶手段を備え、前記出力手段は、さらに、前記訪問者情報を、前記入出力装置を介して前記認証装置へ出力するとしてもよい。

この構成によると、記録媒体は、訪問者に係る訪問者情報を記憶し、記憶している訪問者情報を認証装置へ出力することができる。

[0054] ここで、前記認証装置は、前記証明情報の正当性を認証する認証情報を記憶しており、前記認証装置及び前記記録媒体は、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行うとしてもよい。

この構成によると、記録媒体は、証明情報と認証情報とを用いたチャレンジレスポンス型による認証を行うことができる。

[0055] ここで、前記記録媒体は、携帯電話機に装着されるとしてもよい。

この構成によると、記録媒体は、携帯電話機に装着され使用されることができる。

図面の簡単な説明

[0056] [図1]身元認証システム1の全体の概要を示す図である。

[図2]認証カード10の構成を示すブロック図である。

[図3]ユーザ端末20及びカードリーダ30の構成を示すブロック図である。

[図4]認証鍵記憶部201が有する鍵情報テーブルT100のデータ構造を示す。

[図5]身元認証システム1における身元認証処理の動作を示す流れ図である。

[図6]身元認証システム1における認証処理の動作を示す流れ図である。

[図7]身元認証システム1Aの全体の概要を示す図である。

[図8]配信装置50Aの構成を示すブロック図である。

[図9]配信鍵記憶部501Aが有する配信鍵情報テーブルT200のデータ構造を示す。

[図10]認証カード10Aの構成を示すブロック図である。

[図11]ユーザ端末20A及びカードリーダ30Aの構成を示すブロック図である。

[図12]身元認証システム1Aにおける配信処理の動作を示す流れ図である。

[図13]身元認証システム1Aにおける身元認証処理の動作を示す流れ図である。

[図14]身元認証システム1Aにおける認証処理の動作を示す流れ図である。

[図15]身元認証システム1Bの全体の概要を示す図である。

[図16]認証カード10Bの構成を示すブロック図である。

[図17]ユーザ端末20B及びカードリーダ30Bの構成を示すブロック図である。

[図18]身元認証システム1Bにおける身元認証処理の動作を示す流れ図である。

[図19]身元認証システム1Bにおける認証処理の動作を示す流れ図である。

[図20]身元認証システム1Cの全体の概要を示す図である。

[図21]配信装置50Cの構成を示すブロック図である。

[図22]認証カード10Cの構成を示すブロック図である。

[図23]訪問鍵記憶部105Cが有する証明用訪問情報テーブルT300及び証明用訪問鍵テーブルT310のデータ構造を示す。

[図24]ユーザ端末20C及びカードリーダ30Cの構成を示すブロック図である。

[図25]身元認証システム1Cにおける訪問情報配信処理の動作を示す流れ図である。

[図26]身元認証システム1Cにおける身元認証処理の動作を示す流れ図である。図27へ続く。

[図27]身元認証システム1Cにおける身元認証処理の動作を示す流れ図である。図26から続く。

[図28]身元認証システム1Cにおける訪問鍵認証処理の動作を示す流れ図である。

[図29]身元認証システム1Cにおける訪問情報検証処理の動作を示す流れ図である。

[図30]身元認証システム1Dの全体の概要を示す図である。

[図31]認証カード10D及び第2入出力装置70Dの構成を示すブロック図である。

[図32]ユーザ端末20D及び第1入出力装置60Dの構成を示すブロック図である。

[図33]鍵情報テーブルT500のデータ構造を示す。

[図34]情報テーブルT600のデータ構造を示す。

[図35]認証カード1010の構成を示すブロック図である。

[図36]ユーザ端末1020及びカードリーダ1030の構成を示すブロック図である。

[図37]身元認証システム1000における身元認証処理の動作を示す流れ図である。

[図38]身元認証システム1000における検証処理の動作を示す流れ図である。

[図39]身元認証システム1000における認証処理の動作を示す流れ図である。

符号の説明

[0057] 1 身元認証システム

10 認証カード

20 ユーザ端末

30 カードリーダ

40 ケーブル

101 証明鍵記憶部

102 制御部

103 入出力部

201 認証鍵記憶部

202 認証部

203 表示部

204 入出力部

250 乱数記憶領域

251 ID記憶領域

290 受話器

300 施錠状態検出部

301 カード読取部

302 入出力部

390 呼出ボタン

391 マイク

392 スピーカー

394 装着口

発明を実施するための最良の形態

[0058] 1．第1の実施の形態

本発明に係る第1の実施の形態としての身元認証システム1について説明する。

1．1 身元認証システム1の概要

身元認証システム1は、図1に示すように、認証カード10とユーザ端末20とカードリーダ30とから構成されている。

[0059] 認証カード10は、利用者宅へ訪問する訪問業者（例えば、宅配便の業者）が所有するカードである。認証カード10には、認証カード10自身の正当性を証明するための訪問業者固有の身元証明鍵を予め記憶している。身元証明鍵は、訪問業者にて安全に管理されている。なお、認証カードにて記憶される身元証明鍵は、訪問業者毎に異なる。つまり、認証カード10を所有する訪問業者と異なる訪問業者は、認証カード10に記憶されている身元証明鍵とは異なる身元証明鍵が予め記憶されている認証カード11（図示せず）を所有している。

[0060] なお、身元証明鍵は、訪問業者毎に異なるとしたが、同一の訪問業者に属する各訪問者が所有する認証カード毎に異なるとしてもよい。このとき、訪問業者は、各認証カード自身の正当性を証明するための訪問業者固有の各身元証明鍵を、安全に

管理に管理している。

ユーザ端末20及びカードリーダ30は、訪問業者から配布された装置であり、ユーザ端末20には、認証カード10の正当性を検証するための身元認証鍵が予め記憶されている。

[0061] ユーザ端末20は、利用者の宅内に配置されており、具体的には、インターホンの親機である。カードリーダ30は、認証カード10の着脱が可能であり、利用者の宅外(例えば、玄関先)に配置されており、具体的には、装着された認証カード10に対して、情報の入出力を行うカードリーダライタの機能を備えたインターホンの子機である。ユーザ端末20とカードリーダ30とは、ケーブル40にて接続されている。ユーザ端末20は、受話器290を備え、インターホンの親機としての機能動作を行う。カードリーダ30は、呼出ボタン390、マイク391及びスピーカー392を備えており、インターホンの子機としての機能動作を行う。例えば、訪問者は、カードリーダ30の呼出ボタン390を押下して、宅内にいる利用者を呼び出し、利用者は、受話器290を用い、訪問者は、マイク391及びスピーカー392を用いて、インターホン越しに会話を行う。

[0062] ここで、認証カード10とユーザ端末20とカードリーダ30とを用いて、身元認証システム1の動作の概要について説明する。

身元認証システム1は、認証カード10がカードリーダ30の装着口394に挿入されると、認証カード10に記憶している身元証明鍵と、ユーザ端末20に記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末20の表示部203にて表示する。

[0063] 利用者は、訪問者に対して、玄関のドアを施錠している状態で、認証カード10をカードリーダ30に装着させることができる。また、利用者は、ユーザ端末20による認証の結果により、玄関のドアの施錠を解除するか否かを決定することができる。つまり、利用者は、認証結果が肯定的である場合には、玄関のドアを開け、認証結果が否定的である場合には、玄関のドアを開けないようにすることができる。

[0064] なお、ここで用いる暗号処理は、秘密鍵による暗号処理である。秘密鍵による暗号処理の一例は、DESである。DESについては、公知であるので説明を省略するが、身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。

また、身元認証システム1において、認証カード11（図示せず）がカードリーダ30に挿入された場合も同様の動作を行うため、以降では、認証カード10を用いて説明する。

[0065] 1．2 認証カード10の構成

ここでは、認証カード10の構成について説明する。認証カード10は、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10は、図2に示すように、証明鍵記憶部101、制御部102及び入出力部103から構成されている。

[0066] 認証カード10は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10は、その機能を達成する。

（1） 証明鍵記憶部101

証明鍵記憶部101は、耐タンパ性を有しており、身元証明鍵と、身元証明鍵を識別する証明鍵IDとからなる組を1つ記憶している。

[0067] 以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

（2） 制御部102

制御部102は、カードリーダ30より入出力部103を介して、証明鍵IDを要求する旨のID要求情報を受け取ると、証明鍵記憶部101より証明鍵IDを取得し、取得した証明鍵IDを入出力部103を介してカードリーダ30へ出力する。

[0068] さらに、制御部102は、カードリーダ30より乱数「N」を受け取ると、証明鍵記憶部101より身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダ30より受け取った乱数「N」に対して暗号化を施し、暗号化情報Enc（SK1、N）を生成する。制御部102は、生成した暗号化情報を入出力部103を介してカードリーダ30へ出力する。ここで、Enc（SK1、N）は、乱数「N」が身元証明鍵「SK1」にて暗号化された情報であることを意味する。

[0069] （3） 入出力部103

入出力部103は、カードリーダ30より受け取った情報を制御部102へ出力し、制御部102から受け取った情報をカードリーダ30へ出力する。

1．3 ユーザ端末20の構成

ここでは、ユーザ端末20の構成について説明する。ユーザ端末20は、カードリーダ30に挿入された認証カード10の認証を行う。ユーザ端末20は、図3に示すように、認証鍵記憶部201、認証部202、表示部203及び入出力部204から構成されている。

[0070] ユーザ端末20は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20は、その機能を達成する。

[0071] なお、ユーザ端末20におけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

（1） 認証鍵記憶部201

認証鍵記憶部201は、耐タンパ性を有しており、図4に一例として示すように、鍵情報テーブルT100を備えている。

[0072] 鍵情報テーブルT100は、身元認証鍵と認証鍵IDとからなる組を複数記憶するための領域を備えている。

身元認証鍵は、カードリーダ30の挿入された認証カードの正当性を検証するための鍵であり、上述したように身元証明鍵と同一のものである。

認証鍵IDは、身元認証鍵を識別する識別子であり、証明鍵IDと同一の識別子にて対応付けされている。これにより、身元認証鍵と身元証明鍵との対応付けが可能となる。

[0073] また、鍵情報テーブルT100にて記憶されている身元認証鍵の個数は、訪問業者の数と同じ数である。

つまり、認証カード10、11、・・・、12のそれぞれに記憶されている証明鍵IDと身元証明鍵との組に対応する、認証鍵IDと身元認証鍵とからなる組が記憶されている。

[0074] (2) 認証部202

認証部202は、乱数を記憶する乱数記憶領域250及びカードリーダ30より入出力部204を介して受け取った証明鍵IDを記憶するID記憶領域251を有している。

認証部202は、カードリーダ30より入出力部204を介して、カードリーダ30に認証カード10が挿入されたことを検知した旨を示す検知情報と、証明鍵IDとを受け取り、受け取った証明鍵IDをID記憶領域251に記憶する。次に、認証部202は、乱数「N」を生成し、生成した乱数「N」を入出力部204を介してカードリーダ30へ出力し、生成した乱数「N」を乱数記憶領域250に記憶する。

[0075] さらに、認証部202は、カードリーダ30より入出力部204を介して、暗号化情報Enc(SK1、N)を受け取る。次に、ID記憶領域251にて記憶している証明鍵IDと一致する認証鍵IDと対応する身元認証鍵を鍵情報テーブルT100より取得し、取得した身元認証鍵を用いて、暗号化情報Enc(SK1、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250にて記憶している乱数「N」とが一致するか否かを判断する。

[0076] 復号結果と乱数「N」とが一致する場合には、認証部202は、カードリーダ30に挿入された認証カードが正当な認証カードであると認証、つまり挿入された認証カードが正当な認証カードであると決定し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部203へ出力する。復号結果と乱数「N」とが一致しない場合には、認証部202は、カードリーダ30に挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部203へ出力する。さらに、認証部202は、乱数記憶領域250に記憶している乱数「N」の消去、及びID記憶領域251に記憶している証明鍵IDの消去を行う。

[0077] また、認証部202は、ユーザへ玄関ドアの施錠を行う旨の施錠メッセージをカードリーダ30より受け取ると、受け取った施錠メッセージを表示部203へ出力する。

(3) 表示部203

表示部203は、例えば、ディスプレイを備え、認証部202より受け取った認証結果の情報を外部に対して表示する。

[0078] 表示部203は、認証部202より受け取った施錠メッセージを外部に対して表示する。

(4) 入出力部204

入出力部204は、カードリーダ30より受け取った情報を認証部202へ出力し、認証部202から受け取った情報をカードリーダ30へ出力する。

[0079] 1.4 カードリーダ30

カードリーダ30は、図3に示すように、カード読取部301、入出力部302及び施錠状態検出部300から構成されている。

カードリーダ30は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ30は、その機能を達成する。

[0080] なお、カードリーダ30におけるインターホンの子機としての機能については、公知であるため、子機としての構成図及び説明は省略する。

(1) カード読取部301

カード読取部301は、認証カード10が挿入されたことの検知を行う。カード読取部301は、認証カード10が挿入されたことを検知すると、施錠状態の検出する施錠検出命令を施錠状態検出部300へ出力する。

[0081] カード読取部301は、施錠状態検出部300から、玄関ドアが施錠されている状態を検出したことを示す施錠検出情報を受け取ると、検知情報及びID要求情報を生成し、生成したID要求情報を認証カード10へ出力する。次に、認証カード10より証明鍵IDを受け取ると、受け取った証明鍵IDと、生成した検知情報とを入出力部302を介してユーザ端末20へ出力する。

[0082] さらに、カード読取部301は、ユーザ端末20より入出力部302を介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード10へ出力する。カード読取部301は、認証カード10より暗号化情報Enc(SK1、N)を受け取ると、受け取った暗号化情報Enc(SK1、N)を入出力部302を介してユーザ端末20へ出力する。

(2)施錠状態検出部300

施錠状態検出部300は、玄関ドアを施錠する鍵機構と接続されており、玄関ドアの施錠されている状態の検出を行う。

[0083] 施錠状態検出部300は、カード読取部301より施錠検出命令を受け取ると、玄関ドアが施錠状態であるか、開錠状態であるかを判断する。

施錠状態検出部300は、施錠状態であると判断、つまり玄関ドアが施錠されている状態を検出した場合には、施錠検出情報をカード読取部301へ出力する。

施錠状態検出部300は、開錠状態であると判断、つまり施錠されている状態を検出しない場合には、ユーザへ玄関ドアの施錠を行う旨の施錠メッセージを、入出力部302を介してユーザ端末20へ出力する。施錠状態検出部300は、玄関ドアが施錠されている状態を検出するまでの間、施錠メッセージをユーザ端末20へ出力する。

[0084] (3) 入出力部302

入出力部302は、ユーザ端末20より受け取った情報をカード読取部301へ出力し、カード読取部301から受け取った情報をユーザ端末20へ出力する。

入出力部302は、施錠状態検出部300から受け取った施錠メッセージをユーザ端末20へ出力する。

[0085] 1.5 身元認証処理の動作

ここでは、認証カード10がカードリーダ30に挿入されてからユーザ端末20にて認証を行うまでの処理である身元認証処理の動作について、図5に示す流れ図を用いて説明する。

カードリーダ30は、認証カード10が挿入されたことを検知すると(ステップS5)、施錠されている状態を検出する(ステップ8)。なお、施錠されている状態を検出しない場合には、施錠されている状態を検出するまで、待ち受け状態となる。このとき、上述したように、玄関ドアが施錠されるまでの間、ユーザ端末20にて、施錠メッセージが表示されている。

[0086] カードリーダ30は、ステップS8にて、玄関ドアが施錠されている状態を検出すると、検知情報及びID要求情報を生成し、生成したID要求情報を認証カード10へ出力する(ステップS10)。

認証カード10は、カードリーダ30よりID要求情報を受け取ると、証明鍵記憶部101

にて記憶している証明鍵IDを取得し、取得した証明鍵IDをカードリーダ30へ出力する(ステップS15)。

[0087] カードリーダ30は、認証カード10より証明鍵IDを受け取ると(ステップS20)、受け取った証明鍵IDと、ステップS10にて生成した検知情報とをユーザ端末20へ出力する(ステップS25)。

ユーザ端末20は、カードリーダ30より証明鍵IDと検知情報とを受け取ると、受け取った証明鍵IDをID記憶領域251に記憶する(ステップS30)。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」をカードリーダ30へ出力し、さらに、生成した乱数「N」を乱数記憶領域250に記憶する(ステップS35)。

[0088] カードリーダ30は、ユーザ端末20より乱数「N」を受け取ると、受け取った乱数「N」を認証カード10へ出力する(ステップS40)。

認証カード10は、カードリーダ30より乱数「N」を受け取ると(ステップS45)、受け取った乱数「N」を証明鍵記憶部101にて記憶している身元証明鍵を用いて暗号化し、暗号化情報を生成し、生成した暗号化情報をカードリーダ30へ出力する(ステップS50)。

[0089] カードリーダ30は、認証カード10より暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末20へ出力する(ステップS55)。

ユーザ端末20は、カードリーダ30より暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部201にて記憶している身元認証鍵とを用いて、認証処理を行う(ステップS60)。

[0090] 1.6 認証処理

ここでは、身元認証処理のステップS60にて行われる認証処理について、図6に示す流れ図を用いて説明する。

ユーザ端末20は、認証カード10よりカードリーダ30を介して暗号化情報を受け取る(ステップS100)。次に、ユーザ端末20は、身元認証処理のステップS30にてID記憶領域251に記憶した証明鍵IDと一致する認証鍵IDと対応付けられた身元認証鍵を鍵情報テーブルT100より取得する(ステップS105)。さらに、ユーザ端末20は、取得した身元認証鍵を用いて、ステップS100にて受け取った暗号化情報を復号

する(ステップS110)。

[0091] 次に、ユーザ端末20は、復号して得られた復号結果と、身元認証処理のステップS35にて乱数記憶領域250に記憶した乱数「N」とが一致するか否かの判断を行う(ステップS115)。

一致すると判断する場合には(ステップS115における「YES」)、正当訪問者情報を生成し、生成した正当訪問者情報を表示し(ステップS120)、乱数記憶領域250に記憶している乱数「N」、及びID記憶領域251に記憶している証明鍵IDをそれぞれ消去し(ステップS130)、処理を終了する。

[0092] 一致しないと判断する場合には(ステップS115における「NO」)、不正訪問者情報を生成し、生成した不正訪問者情報を表示し(ステップS125)、乱数記憶領域250に記憶している乱数「N」、及びID記憶領域251に記憶している証明鍵IDをそれぞれ消去し(ステップS130)、処理を終了する。

2. 第2の実施の形態

ここでは、本発明に係る第2の実施の形態としての身元認証システム1Aについて説明する。

[0093] 身元認証システム1では、身元認証鍵をユーザ端末20の認証鍵記憶部201に予め記憶したが、身元認証システム1Aでは、ユーザ端末が利用者に配布された後に、訪問業者より身元認証鍵を配布する。

2. 1 身元認証システム1Aの概要

身元認証システム1Aは、図7に示すように、認証カード10Aと、ユーザ端末20Aと、カードリーダ30Aと、配信装置50Aとから構成されている。カードリーダ30Aとユーザ端末20Aとは、ケーブル40Aにて接続されている。

[0094] ユーザ端末20Aは、利用者の宅内に配置されており、具体的には、インターホンの親機である。カードリーダ30Aは、認証カード10Aの着脱が可能であり、利用者の宅外(例えば、玄関先)に配置されており、具体的には、装着された認証カード10Aに対して、情報の入出力を行うカードリーダライタの機能を備えたインターホンの子機である。ユーザ端末20Aは、受話器290Aを備え、インターホンの親機としての機能動作を行う。カードリーダ30Aは、呼出ボタン390A、マイク391A及びスピーカー392

Aを備えており、インターホンの子機としての機能動作を行う。例えば、訪問者は、カードリーダ30Aの呼出ボタン390Aを押下して、宅内にいる利用者を呼び出し、利用者は、受話器290Aを用い、訪問者は、マイク391A及びスピーカー392Aを用いて、インターホン越しに会話を行う。

[0095] 認証カード10Aは、訪問業者より利用者宅へ訪問する訪問者に割り当てられており、身元証明鍵を予め記憶している。なお、認証カードにて記憶される身元証明鍵は、訪問者毎に異なる。つまり、認証カード10Aを所有する訪問者と異なる訪問者は、認証カード10Aに記憶されている身元証明鍵とは異なる身元証明鍵が予め記憶されている認証カード11A(図示せず)を所有している。これにより、利用者宅へ訪問する訪問者と身元証明鍵とが対応付けられていることになる。

[0096] ここで、図7には図示していないが、ユーザ端末20Aと同様の構成を有するユーザ端末21A、・・・、22Aも配信装置50Aとインターネットを介して接続されている。また、ユーザ端末21A、・・・、22Aはカードリーダ30Aと同様の構成を有するカードリーダ31A、・・・、32Aとそれぞれ接続されている。

ここでは、認証カード10Aとユーザ端末20Aとカードリーダ30Aとを用いて、身元認証システム1Aの概要について説明する。なお、ユーザ端末21A、・・・、22Aは、ユーザ端末20Aと同様であり、カードリーダ31A、・・・、32Aは、カードリーダ30Aと同様であるため、説明は省略する。

[0097] 身元認証システム1Aでは、訪問業者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末20Aへインターネットを介して送信する。認証カード10Aがカードリーダ30Aの装着口394Aに挿入されると、ユーザ端末20Aは、認証カード10Aに記憶されている身元証明鍵と、配信装置50Aより事前に受信して記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果を表示部203Aにて表示する。

[0098] 利用者は、訪問者に対して、玄関のドアを施錠している状態で、認証カード10をカードリーダ30に装着させることができる。また、利用者は、ユーザ端末20による認証の結果により、玄関のドアの施錠を解除するか否かを決定することができる。つまり、利用者は、認証結果が肯定的である場合には、玄関のドアを開け、認証結果が否定

的である場合には、玄関のドアを開けないようにすることができる。

[0099] ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。

また、身元認証システム1Aにおいて、認証カード11A(図示せず)がカードリーダ30Aに挿入された場合も同様の動作を行うため、以降では、認証カード10Aを用いて説明する。

[0100] 2.2 配信装置50A

配信装置50Aは、訪問者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末20Aへ送信する装置である。配信装置50Aは、図8に示すように、配信鍵記憶部501A、制御部502A、操作部503A及び送信部504Aから構成されている。

[0101] 配信装置50Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどからなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置50Aは、その機能を達成する。

[0102] (1) 配信鍵記憶部501A

配信鍵記憶部501Aは、図9に一例として示すように、配信鍵情報テーブルT200を備えている。

配信鍵情報テーブルT200は、訪問者IDと身元認証鍵とからなる組を複数記憶するための領域を備えている。

[0103] 訪問者IDは、訪問者を識別する識別子であり、身元認証鍵は、身元証明鍵と同一の鍵であり、訪問者IDと対応付けられている。

なお、ここで記憶されている身元認証鍵の個数は、訪問者の人数、つまり認証カードの個数と同一となる。

また、身元認証鍵と訪問者IDとを対応付けることにより、訪問者IDに対応する身元認証鍵を記憶している認証カードを訪問者に割り当てることができる。

[0104] (2) 制御部502A

制御部502Aは、操作部503Aより、身元認証鍵の登録を示す情報と、訪問者IDと、身元認証鍵とを受け取ると、受け取った訪問者IDと身元認証鍵とを対応付けて、配信鍵記憶部501Aへ書き込む。

制御部502Aは、操作部503Aより身元認証鍵をユーザ端末20Aへ配信する旨の情報と、訪問者IDとからなる配信情報を受け取ると、受け取った配信情報に含まれる訪問者IDと対応する身元認証鍵を配信鍵情報テーブルT200より取得する。制御部502Aは、取得した身元認証鍵をユーザ端末20Aへ送信部504Aを介して送信する。

[0105] (3) 操作部503A

操作部503Aは、配信装置50Aの操作者の操作により、身元認証鍵の登録を示す情報と、訪問者IDと、身元認証鍵とを受け付けると、受け付けた身元認証鍵の登録を示す情報と、訪問者IDと、身元認証鍵とを制御部502Aへ出力する。

また、操作部503Aは、操作者の操作により、配信情報を受け付けると、受け付けた配信情報を制御部502Aへ出力する。

[0106] なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。

(4) 送信部504A

送信部504Aは、制御部502Aより受け取った情報をユーザ端末20Aへインターネットを介して出力する。

[0107] 2.3 認証カード10A

ここでは、認証カード10Aの構成について説明する。認証カード10Aは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10Aは、図10に示すように、証明鍵記憶部101A、制御部102A及び入出力部103Aから構成されている。

[0108] 認証カード10Aは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作すること

により、認証カード10Aは、その機能を達成する。

（1） 証明鍵記憶部101A

証明鍵記憶部101Aは、耐タンパ性を有しており、訪問者に対応する身元証明鍵を1つ記憶している。

[0109] 以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

（2） 制御部102A

制御部102Aは、カードリーダ30Aより乱数「N」を受け取ると、証明鍵記憶部101Aより身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダ30Aより受け取った乱数「N」に対して暗号化を施し、暗号化情報Enc（SK1、N）を生成する。制御部102Aは、生成した暗号化情報を入出力部103Aを介してカードリーダ30Aへ出力する。

[0110] （3） 入出力部103A

入出力部103Aは、認証カード10の入出力部103と同様であるため、説明は省略する。

2．4 ユーザ端末20Aの構成

ここでは、ユーザ端末20Aの構成について説明する。ユーザ端末20Aは、図11に示すように、認証鍵記憶部201A、認証部202A、表示部203A、入出力部204A及び受信部205Aから構成されている。

[0111] ユーザ端末20Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Aは、その機能を達成する。

[0112] また、上記の身元認証システム1Aの概要にて示したように、ユーザ端末21A、・・・、22Aは、ユーザ端末20Aと同様の構成であるため、説明は省略する。

なお、ユーザ端末20Aにおけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

（1） 認証鍵記憶部201A

認証鍵記憶部201Aは、耐タンパ性を有しており、配信装置50Aよりインターネットを介して受信した身元認証鍵を記憶する領域を有している。

[0113] （2） 受信部205A

受信部205Aは、配信装置50Aよりインターネットを介して、身元認証鍵を受信すると、受信した身元認証鍵を認証鍵記憶部201Aへ書き込む。

これにより、ユーザ端末20Aは、訪問者に対応する身元認証鍵を事前に記憶することができる。

[0114] （3） 認証部202A

認証部202Aは、乱数を記憶する乱数記憶領域250Aを有している。

認証部202Aは、カードリーダ30Aより入出力部204Aを介して、カードリーダ30Aに認証カード10Aが挿入されたことを検知した旨を示す検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」を入出力部204Aを介してカードリーダ30Aへ出力し、生成した乱数「N」を乱数記憶領域250Aに記憶する。

[0115] さらに、認証部202Aは、カードリーダ30Aより入出力部204Aを介して、暗号化情報Enc（SK1、N）を受け取ると、認証鍵記憶部201Aにて事前に記憶している身元認証鍵を認証鍵記憶部201Aより取得し、取得した身元認証鍵を用いて、暗号化情報Enc（SK1、N）の復号を行い、復号により得られた復号結果と、乱数記憶領域250Aにて記憶している乱数「N」とが一致するか否かを判断する。

[0116] 復号結果と乱数「N」とが一致する場合には、認証部202Aは、カードリーダ30Aに挿入された認証カードが正当な認証カードであると認証、つまり挿入された認証カードが正当な認証カードであると決定し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部203Aへ出力する。復号結果と乱数「N」とが一致しない場合には、認証部202Aは、カードリーダ30Aに挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Aへ出力する。さらに、認証部202Aは、認証鍵記憶部201Aにて記憶している身元認証鍵の消去及び乱数記憶領域250Aに記憶している乱

数「N」の消去を行う。

[0117] (4) 表示部203A

表示部203Aは、ユーザ端末20の表示部203と同様であるため、説明は省略する。

(5) 入出力部204A

入出力部204Aは、ユーザ端末20の入出力部204と同様であるため、説明は省略する。

[0118] 2.5 カードリーダ30A

カードリーダ30Aは、図11に示すように、カード読取部301A及び入出力部302Aから構成されている。

カードリーダ30Aは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ30Aは、その機能を達成する。

[0119] なお、上記の身元認証システム1Aの概要にて示したように、カードリーダ31A、・・・、32Aは、カードリーダ30Aと同様の構成であるため、説明は省略する。

なお、カードリーダ30Aにおけるインターホンの子機としての機能については、公知であるため、子機としての構成図及び説明は省略する。

(1) カード読取部301A

カード読取部301Aは、認証カード10Aが挿入されたことの検知を行う。カード読取部301Aは、認証カード10Aが挿入されたことを検知すると、検知情報を生成し、生成した検知情報を入出力部302Aを介してユーザ端末20Aへ出力する。

[0120] さらに、カード読取部301Aは、ユーザ端末20Aより入出力部302Aを介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード10Aへ出力する。カード読取部301Aは、認証カード10Aより暗号化情報Enc(SK1、N)を受け取ると、受け取った暗号化情報Enc(SK1、N)を入出力部302Aを介してユーザ端末20Aへ出力する。

[0121] (2) 入出力部302A

入出力部302Aは、カードリーダ30の入出力部302と同様であるため、説明は省略

する。

2．6 配信処理の動作

ここでは、身元認証鍵を事前に配信する配信処理について、図12に示す流れ図を用いて、説明する。

[0122] 配信装置50Aは、利用者の操作により配信情報を受け付けると(ステップS200)、受け付けた配信情報に含まれる訪問者IDに対応する身元認証鍵を配信鍵記憶部501Aより取得する(ステップS205)。次に、配信装置50Aは、取得した身元認証鍵をユーザ端末20Aへインターネットを介して配信する(ステップS210)。

ユーザ端末20Aは、配信装置50Aより身元認証鍵を受信すると(ステップS215)、受信した身元認証鍵を認証鍵記憶部201Aへ書き込む(ステップS220)。

[0123] 2．7 身元認証処理の動作

ここでは、認証カード10Aがカードリーダ30Aに挿入されてからユーザ端末20Aにて認証を行うまでの処理である身元認証処理の動作について、図13に示す流れ図を用いて説明する。

カードリーダ30Aは、認証カード10Aが挿入されたことを検知すると(ステップS250)、検知情報を生成し、生成した検知情報をユーザ端末20Aへ出力する(ステップS255)。

[0124] ユーザ端末20Aは、カードリーダ30Aより検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」をカードリーダ30Aへ出力し、さらに、生成した乱数「N」を乱数記憶領域250Aに記憶する(ステップS260)。

カードリーダ30Aは、ユーザ端末20Aより乱数「N」を受け取ると、受け取った乱数「N」を認証カード10Aへ出力する(ステップS265)。

[0125] 認証カード10Aは、カードリーダ30Aより乱数「N」を受け取ると(ステップS270)、受け取った乱数「N」を証明鍵記憶部101Aにて記憶している身元証明鍵を用いて暗号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダ30Aへ出力する(ステップS275)。

カードリーダ30Aは、認証カード10Aより暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末20Aへ出力する(ステップS280)。

[0126] ユーザ端末20Aは、カードリーダ30Aより暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部201Aにて記憶している身元認証鍵とを用いて、認証処理を行う(ステップS285)。

2．8 認証処理

ここでは、身元認証処理のステップS285にて行われる認証処理について、図14に示す流れ図を用いて説明する。

[0127] ユーザ端末20Aは、認証カード10Aよりカードリーダ30Aを介して暗号化情報を受け取る(ステップS300)。次に、ユーザ端末20Aは、配信装置50Aより事前に配信された身元認証鍵を認証鍵記憶部201Aより取得する(ステップS305)。さらに、ユーザ端末20Aは、取得した身元認証鍵を用いて、ステップS300にて受け取った暗号化情報を復号する(ステップS310)。

[0128] 次に、ユーザ端末20Aは、復号して得られた復号結果と、身元認証処理のステップS260にて乱数記憶領域250Aに記憶した乱数「N」とが一致するか否かの判断を行う(ステップS315)。

一致すると判断する場合には(ステップS315における「YES」)、正当訪問者情報を生成し、生成した正当訪問者情報を表示し(ステップS320)、認証鍵記憶部201Aにて記憶している身元認証鍵及び乱数記憶領域250Aに記憶している乱数「N」を消去し(ステップS330)、処理を終了する。

[0129] 一致しないと判断する場合には(ステップS315における「NO」)、不正訪問者情報を生成し、生成した不正訪問者情報を表示し(ステップS325)、認証鍵記憶部201Aにて記憶している身元認証鍵及び乱数記憶領域250Aに記憶している乱数「N」を消去し(ステップS330)、処理を終了する。

3．第3の実施の形態

ここでは、本発明に係る第3の実施の形態としての身元認証システム1Bについて説明する。

[0130] 身元認証システム1Bでは、訪問者が利用者宅に訪問時に、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行う。

3．1　身元認証システム1Bの概要

身元認証システム1Bは、図15に示すように、認証カード10Bとユーザ端末20Bとカードリーダ30Bとから構成されている。カードリーダ30Bとユーザ端末20Bとは、ケーブル40Bにて接続されている。

[0131] ユーザ端末20Bは、利用者の宅内に配置されており、具体的には、インターホンの親機である。カードリーダ30Bは、認証カード10Bの着脱が可能であり、利用者の宅外（例えば、玄関先）に配置されており、具体的には、装着された認証カード10Bに対して、情報の入出力を行うカードリーダライタの機能を備えたインターホンの子機である。ユーザ端末20Bは、受話器290Bを備え、インターホンの親機としての機能動作を行う。カードリーダ30Bは、呼出ボタン390B、マイク391B及びスピーカー392Bを備えており、インターホンの子機としての機能動作を行う。例えば、訪問者は、カードリーダ30Bの呼出ボタン390Bを押下して、宅内にいる利用者を呼び出し、利用者は、受話器290Bを用い、訪問者は、マイク391B及びスピーカー392Bを用いて、インターホン越しに会話を行う。

[0132] 認証カード10Bは、訪問業者より利用者宅へ訪問する訪問者に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は訪問者の指紋模様の特徴点からなる身元証明指紋情報とする。なお、認証カードにて記憶される身元証明鍵は、訪問者毎に異なる。つまり、認証カード10Bを所有する訪問者と異なる訪問者は、認証カード10Bに記憶されている身元証明鍵とは異なる身元証明鍵が予め記憶されている認証カード11B（図示せず）を所有している。

[0133] カードリーダ30Bは、訪問者より指紋の入力を受け付ける指紋読取部310Bを有している。

ここで、認証カード10Bとユーザ端末20Bとカードリーダ30Bとを用いて、身元認証システム1Bの動作の概要について説明する。

身元認証システム1Bは、認証カード10Bがカードリーダ30Bの装着口394Bに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム1Bは、カードリーダ30Bの指紋読取部310Bより指紋の入力を受け付けると、受け付けた指紋より

指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード10Bに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末20Bの表示部203Bにて表示する。

[0134] 利用者は、訪問者に対して、玄関のドアを施錠している状態で、認証カード10をカードリーダ30に装着させることができる。また、利用者は、ユーザ端末20による認証の結果により、玄関のドアの施錠を解除するか否かを決定することができる。つまり、利用者は、認証結果が肯定的である場合には、玄関のドアを開け、認証結果が否定的である場合には、玄関のドアを開けないようにすることができる。

[0135] ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明鍵と身元認証指紋情報とが同一の鍵となることは、言うまでもない。

また、身元認証システム1Bにおいて、認証カード11B(図示せず)がカードリーダ30Bに挿入された場合も同様の動作を行うため、以降では、認証カード10Bを用いて説明する。

[0136] なお、正当な訪問者に対して、認証カード10Bに記憶している身元証明鍵と、カードリーダ30Bにて生成した身元認証指紋情報とが、常に一致する必要があるが、指紋を常に一意なユニークな指紋情報に変換する方法が開示されており、公知の技術であるため、ここでは、説明を省略する。なお、柴田陽一他著による「メカニズムPKI」(コンピュータセキュリティシンポジウム2003, p181−186, 2003.)にて、変換方法についての詳細な記述がある。

[0137] 3.2 認証カード10B

ここでは、認証カード10Bの構成について説明する。認証カード10Bは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10Bは、図16に示すように、証明鍵記憶部101B、制御部102B及び入出力部103Bから構成されている。

[0138] 認証カード10Bは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶され

ている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10Bは、その機能を達成する。

（1） 証明鍵記憶部101B

証明鍵記憶部101Bは、耐タンパ性を有しており、訪問者に対応する身元証明指紋情報を身元証明鍵として1つ記憶している。

[0139] 以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

（2） 制御部102B

制御部102Bは、第2の実施の形態にて示した認証カード10Aの制御部102Aと同様であるため、説明は省略する。

（3） 入出力部103B

入出力部103Bは、第2の実施の形態にて示した認証カード10Aの入出力部103Aと同様であるため、説明は省略する。つまり、入出力部103Bは、第1の実施の形態にて示した認証カード10の入出力部103とも同様である。

[0140] 3．3 ユーザ端末20Bの構成

ここでは、ユーザ端末20Bの構成について説明する。ユーザ端末20Bは、図17に示すように、認証鍵記憶部201B、認証部202B、表示部203B及び入出力部204Bとから構成されている。

ユーザ端末20Bは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Bは、その機能を達成する。

[0141] なお、ユーザ端末20Bにおけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

（1） 認証鍵記憶部201B

認証鍵記憶部201Bは、耐タンパ性を有しており、身元認証指紋情報を記憶する領域を備えている。

[0142] (2) 認証部202B

認証部202Bは、乱数を記憶する乱数記憶領域250Bを有している。

認証部202Bは、カードリーダ30Bより入出力部204Bを介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダ30Bに認証カード10Bが挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む。次に、認証部202Bは、乱数「N」を生成し、生成した乱数「N」を入出力部204Bを介してカードリーダ30Bへ出力し、生成した乱数「N」を乱数記憶領域250Bに記憶する。

[0143] さらに、認証部202Bは、カードリーダ30Bより入出力部204Bを介して、暗号化情報Enc(SK1、N)を受け取ると、認証鍵記憶部201Bにて記憶している身元認証指紋情報を取得して、取得した身元認証指紋情報を用いて、暗号化情報Enc(SK1、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Bにて記憶している乱数「N」とが一致するか否かを判断する。

[0144] 復号結果と乱数「N」とが一致する場合には、認証部202Bは、カードリーダ30Bに挿入された認証カードが正当な認証カードであると認証、つまり挿入された認証カードが正当な認証カードであると決定し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部203Bへ出力する。復号結果と乱数「N」とが一致しない場合には、認証部202Bは、カードリーダ30Bに挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Bへ出力する。さらに、認証部202Bは、認証鍵記憶部201Bにて記憶している身元認証指紋情報、及び乱数記憶領域250Bにて記憶している乱数「N」の消去を行う。

[0145] (3) 表示部203B

表示部203Bは、第2の実施の形態にて示したユーザ端末20Aの表示部203Aと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したユーザ端末20の表示部203とも同様である。

(4) 入出力部204B

入出力部204Bは、第2の実施の形態にて示したユーザ端末20Aの入出力部204Aと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したユーザ端末20の入出力部204とも同様である。

[0146] 3．4 カードリーダ30B

カードリーダ30Bは、図17に示すように、カード読取部301B、入出力部302B、表示部303B及び指紋読取部310Bから構成されている。

カードリーダ30Bは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ30Bは、その機能を達成する。

[0147] なお、カードリーダ30Bにおけるインターホンの子機としての機能については、公知であるため、子機としての構成図及び説明は省略する。

（1） カード読取部301B

カード読取部301Bは、認証カード10Bが挿入されたことの検知を行う。カード読取部301Bは、認証カード10Bが挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部303Bへ出力する。次に、カード読取部301Bは、指紋読取部310Bより身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部310Bより受け取った身元認証指紋情報とを入出力部302Bを介してユーザ端末20Bへ出力する。

[0148] さらに、カード読取部301Bは、ユーザ端末20Bより入出力部302Bを介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード10Bへ出力する。カード読取部301Bは、認証カード10Bより暗号化情報Enc（SK1、N）を受け取ると、受け取った暗号化情報Enc（SK1、N）を入出力部302Bを介してユーザ端末20Bへ出力する。

[0149] （2） 表示部303B

表示部303Bは、例えば、ディスプレイを備え、カード読取部301Bより要求情報を受け取ると、受け取った要求情報を表示する。これにより、訪問者へ指紋の入力を促すことができる。

（3） 指紋読取部310B

指紋読取部310Bは、指紋センサーから構成され、指紋センサーにより、訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報をカード読取部301Bへ出力する。

[0150] ここで、指紋模様の特徴点とは、隆線の端点や分岐点の方向や位置関係である。

(4) 入出力部302B

入出力部302Bは、第2の実施の形態にて示したカードリーダ30Aの入出力部302Aと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したカードリーダ30の入出力部302とも同様である。

[0151] 3.5 身元認証処理の動作

ここでは、認証カード10Bがカードリーダ30Bに挿入されてからユーザ端末20Bにて認証を行うまでの処理である身元認証処理の動作について、図18に示す流れ図を用いて説明する。

カードリーダ30Bは、認証カード10Bが挿入されたことを検知すると(ステップS400)、要求情報を生成し、生成した要求情報を表示する(ステップS405)。次にカードリーダ30Bは、訪問者より入力された指紋より身元認証指紋情報を生成し(ステップS410)、さらに、検知情報を生成し(ステップS415)、ステップS410にて生成した身元認証指紋情報と、ステップS415にて生成した検知情報とをユーザ端末20Bへ出力する(ステップS420)。

[0152] ユーザ端末20Bは、カードリーダ30Bより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む(ステップS425)。次に、ユーザ端末20Bは、乱数「N」を生成し、生成した乱数「N」をカードリーダ30Bへ出力し、さらに、生成した乱数「N」を乱数記憶領域250Bに記憶する(ステップS430)。

[0153] カードリーダ30Bは、ユーザ端末20Bより乱数「N」を受け取ると、受け取った乱数「N」を認証カード10Bへ出力する(ステップS435)。

認証カード10Bは、カードリーダ30Bより乱数「N」を受け取ると(ステップS440)、受け取った乱数「N」を証明鍵記憶部101Bにて記憶している身元証明鍵を用いて暗

号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダ30Bへ出力する(ステップS445)。

[0154] カードリーダ30Bは、認証カード10Bより暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末20Bへ出力する(ステップS450)。

ユーザ端末20Bは、カードリーダ30Bより暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部201Bにて記憶している身元認証指紋情報とを用いて、認証処理を行う(ステップS455)。

[0155] 3.6 認証処理の動作

ここでは、身元認証処理のステップS455にて行われる認証処理について、図19に示す流れ図を用いて説明する。

ユーザ端末20Bは、認証カード10Bよりカードリーダ30Bを介して暗号化情報を受け取る(ステップS500)。次に、ユーザ端末20Bは、身元認証指紋情報を認証鍵記憶部201Bより取得する(ステップS505)。さらに、ユーザ端末20Bは、取得した身元認証指紋情報を用いて、ステップS500にて受け取った暗号化情報を復号する(ステップS510)。

[0156] 次に、ユーザ端末20Bは、復号して得られた復号結果と、身元認証処理のステップS430にて乱数記憶領域250Bに記憶した乱数「N」とが一致するか否かの判断を行う(ステップS515)。

一致すると判断する場合には(ステップS515における「YES」)、正当訪問者情報を生成し、生成した正当訪問者情報を表示し(ステップS520)、認証鍵記憶部201Bにて記憶している身元認証指紋情報及び乱数記憶領域250Bにて記憶している乱数「N」を消去し(ステップS530)、処理を終了する。

[0157] 一致しないと判断する場合には(ステップS515における「NO」)、不正訪問者情報を生成し、生成した不正訪問者情報を表示し(ステップS525)、認証鍵記憶部201Bにて記憶している身元認証指紋情報及び乱数記憶領域250Bに記憶している乱数「N」を消去し(ステップS530)、処理を終了する。

4. 第4の実施の形態

ここでは、本発明に係る第4の実施の形態としての身元認証システム1Cについて

説明する。

[0158] 身元認証システム1Cでは、以下の動作を行う。

訪問者が利用者宅へ訪問する前に、訪問に係る情報を利用者宅のユーザ端末へ送信し、送信した情報と同様の情報を認証カードへ記憶しておく。訪問時に、先ず、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行い、正当な認証カードであると判断する場合に、訪問者による訪問が正しいものであるかを判断するために、認証カードにて記憶している訪問に係る情報と事前に送信した情報とが同一であるか否かを判断する。

[0159] 4．1 身元認証システム1Cの概要

身元認証システム1Cは、図20に示すように、認証カード10Cと、ユーザ端末20Cと、カードリーダ30Cと、配信装置50Cとから構成されている。カードリーダ30Cとユーザ端末20Cとは、ケーブル40Cにて接続されている。

ユーザ端末20Cは、利用者の宅内に配置されており、具体的には、インターホンの親機である。カードリーダ30Cは、認証カード10Cの着脱が可能であり、利用者の宅外（例えば、玄関先）に配置されており、具体的には、装着された認証カード10Cに対して、情報の入出力を行うカードリーダライタの機能を備えたインターホンの子機である。ユーザ端末20Cは、受話器290Cを備え、インターホンの親機としての機能動作を行う。カードリーダ30Cは、呼出ボタン390C、マイク391C及びスピーカー392Cを備えており、インターホンの子機としての機能動作を行う。例えば、訪問者は、カードリーダ30Cの呼出ボタン390Cを押下して、宅内にいる利用者を呼び出し、利用者は、受話器290Cを用い、訪問者は、マイク391C及びスピーカー392Cを用いて、インターホン越しに会話を行う。

[0160] 認証カード10Cは、訪問業者より利用者宅へ訪問する訪問者に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は訪問者の指紋模様の特徴点からなる身元証明指紋情報とする。なお、認証カードにて記憶される身元証明鍵は、訪問者毎に異なる。つまり、認証カード10Cを所有する訪問者と異なる訪問者は、認証カード10Cに記憶

されている身元証明鍵とは異なる身元証明鍵が予め記憶されている認証カード11C（図示せず）を所有している。

[0161] カードリーダ30Cは、訪問者より指紋の入力を受け付ける指紋読取部310Cを有している。

ここで、図20には、図示していないが、ユーザ端末20Cと同様の構成を有するユーザ端末21C、・・・、22Cも配信装置50Cとインターネットを介して接続されている。また、ユーザ端末21C、・・・、22Cは、カードリーダ30Cと同様の構成を有するカードリーダ31C、・・・、32Cとそれぞれ接続されている。

[0162] ここでは、認証カード10Cとユーザ端末20Cとカードリーダ30Cとを用いて、身元認証システム1Cの概要について説明する。なお、ユーザ端末21C、・・・、22Cは、ユーザ端末20Cと同様であり、カードリーダ31C、・・・、32Cは、カードリーダ30Cと同様であるため、説明は省略する。

身元認証システム1Cでは、配信装置50Cは、訪問業者が利用者宅へ訪問する前に、訪問者による訪問の正当性を検証するために使用する認証用訪問鍵と証明用訪問鍵とを生成、及び訪問時間帯を示す時間情報と訪問内容を示す内容情報とからなる認証用訪問情報を生成する。配信装置50Cは、生成した認証用訪問鍵と、認証用訪問情報とをユーザ端末20Cへインターネットを介して送信する。さらに、配信装置50Cは、送信した認証用訪問情報と同一の内容である証明用訪問情報と、証明用訪問鍵とを、認証用訪問情報及び認証用訪問鍵を送信したユーザ端末を識別する端末IDと対応付けて認証カード10Cにて記憶する。ここで、証明用訪問情報は、訪問時間帯を示す証明用時間情報及び訪問内容を示す証明用内容情報からなる。

[0163] 身元認証システム1Cは、認証カード10Cがカードリーダ30Cの装着口394Cに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム1Cは、カードリーダ30Cの指紋読取部310Cより指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード10Cに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明

鍵と身元認証指紋情報とが同一の鍵となることは、言うまでもない。

[0164] 次に、身元認証システム1Cは、カードリーダ30Cに挿入された認証カードが正当な認証カードであると認証した場合には、証明用訪問鍵の正当性を検証するために、認証用訪問鍵及び証明用訪問鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、秘密鍵による暗号処理であり、証明用訪問鍵と認証用訪問鍵とが同一の鍵となることは、言うまでもない。

[0165] 身元認証システム1Cは、上記認証にて、証明用訪問鍵が正当であると認証した場合には、認証カード10Cにて記憶されている証明用訪問情報に含まれる訪問時間帯及び訪問内容と、事前に送信された認証用訪問情報に含まれる訪問時間帯及び訪問内容とがそれぞれ一致するか否かを判断し、判断結果をユーザ端末20Cの表示部203Cにて表示する。

[0166] 利用者は、訪問者に対して、玄関のドアを施錠している状態で、認証カード10をカードリーダ30に装着させることができる。また、利用者は、ユーザ端末20による認証の結果により、玄関のドアの施錠を解除するか否かを決定することができる。つまり、利用者は、認証結果が肯定的である場合には、玄関のドアを開け、認証結果が否定的である場合には、玄関のドアを開けないようにすることができる。

[0167] また、身元認証システム1Cにおいて、認証カード11C(図示せず)がカードリーダ30Cに挿入された場合も同様の動作を行うため、以降では、認証カード10Cを用いて説明する。

なお、正当な訪問者に対して、認証カード10Cに記憶している身元証明鍵と、カードリーダ30Cにて生成した身元認証指紋情報とが、常に一致する必要があるが、指紋を常に一意なユニークな指紋情報に変換する方法が開示されており、公知の技術であるため、ここでは、説明を省略する。

[0168] 4.2 配信装置50C

配信装置50Cは、訪問者が利用者宅へ訪問する前に、認証用訪問情報をユーザ端末20Cへ送信する装置であり、認証用訪問情報を送信する際には、訪問者に対応する認証カード10Cが配信装置50Cに装着されている。

配信装置50Cは、図21に示すように、端末情報記憶部506C、制御部502C、操

作部503C、送信部504C及び出力部505Cから構成されている。

[0169] 配信装置50Cは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどからなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置50Cは、その機能を達成する。

[0170] (1) 端末情報記憶部506C

端末情報記憶部506Cは、耐タンパ性を有しており、利用者宅へ配布したユーザ端末を一意に識別する端末IDを記憶している。

なお、ここで記憶されている端末IDの個数は、配布したユーザ端末の数と同一となることは言うまでもない。

[0171] (2) 制御部502C

制御部502Cは、操作部503Cより認証用訪問情報をユーザ端末20Cへ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け取ると、認証用訪問鍵及び証明用訪問鍵を生成する。

制御部502Cは、受け取った訪問時間帯及び訪問内容を用いて認証用訪問情報を生成し、生成した認証用訪問情報及び認証用訪問鍵をユーザ端末20Cへ送信する。

[0172] 制御部502Cは、受け取った訪問時間帯及び訪問内容を用いて証明用訪問情報を生成する。さらに、制御部502Cは、ユーザ端末20Cを識別する端末IDを端末情報記憶部506Cより取得し、取得した端末IDと生成した証明用訪問情報と証明用訪問鍵とを対応付けて、出力部505Cを介して認証カード10Cへ出力する。

(3) 操作部503C

操作部503Cは、操作者の操作により、訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると、受け付けた訪問用配信情報と訪問時間帯と訪問内容とを制御部502Cへ出力する。

[0173] なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。

（4） 送信部504C

送信部504Cは、制御部502Cより受け取った情報をユーザ端末20Cへインターネットを介して出力する。

[0174] （5） 出力部505C

出力部505Cは、制御部502Cより受け取った情報を認証カード10Cへ出力する。

4．3 認証カード10C

ここでは、認証カード10Cの構成について説明する。認証カード10Cは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10Cは、図22に示すように、証明鍵記憶部101C、訪問鍵記憶部105C、制御部102C及び入出力部103Cから構成されている。

[0175] 認証カード10Cは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10Cは、その機能を達成する。

（1） 証明鍵記憶部101C

証明鍵記憶部101Cは、耐タンパ性を有しており、訪問者に対応する身元証明指紋情報を身元証明鍵として1つ記憶している。

[0176] 以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

（2） 訪問鍵記憶部105C

訪問鍵記憶部105Cは、耐タンパ性を有しており、図23（a）及び（b）に一例として示すように、証明用訪問情報テーブルT300と、証明用訪問鍵テーブルT310とを備えている。

[0177] 証明用訪問情報テーブルT300は、端末ID、証明用時間情報及び証明用内容情報からなる組を1以上記憶するための領域を備えている。端末IDは、利用者宅に配布したユーザ端末を識別する識別子である。例えば、端末ID「T−ID1」は、ユーザ端末20Cを示し、端末ID「T−ID2」は、ユーザ端末21C（図20では図示せず）を示している。証明用時間情報は、訪問者が訪問する時間帯を示す情報であり、証明用内容

情報は、訪問内容を示す情報である。

[0178] 証明用訪問鍵テーブルT310は、端末ID及び証明用訪問鍵からなる組を1以上記憶するための領域を備えている。端末IDは、上記と同様であり、証明用訪問鍵は、訪問者による訪問の正当性を検証するために使用する鍵である。

(3) 制御部102C

制御部102Cは、配信装置50Cより入出力部103Cを介して端末IDと証明用訪問情報と証明用訪問鍵とを受け取ると、受け取った端末IDと証明用訪問情報とを証明用訪問情報テーブルT300へ書き込む。

[0179] また、制御部102Cは、受け取った端末IDと証明用訪問鍵とを証明用訪問鍵テーブルT310へ書き込む。

また、制御部102Cは、カードリーダ30Cより入出力部103Cを介して、第1乱数「N1」を受け取ると、証明鍵記憶部101Cより身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダ30Cより受け取った第1乱数「N1」に対して暗号化を施し、第1暗号化情報Enc(SK1、N1)を生成する。制御部102Cは、生成した暗号化情報を入出力部103Cを介してカードリーダ30Cへ出力する。

[0180] さらに、制御部102Cは、カードリーダ30Cより入出力部103Cを介して端末ID(例えば、「T—ID1」)と第2乱数「N2」とを受け取ると、受け取った端末IDに対応する証明用訪問鍵「V—key1」を取得し、取得した証明用訪問鍵「V—key1」を用いて、カードリーダ30Cより受け取った第2乱数「N2」に対して暗号化を施し、第2暗号化情報Enc(V—key1、N2)を生成する。制御部102Cは、生成した第2暗号化情報を入出力部103Cを介してカードリーダ30Cへ出力する。また、制御部102Cは、受け取った端末IDを一時的に記憶する。

[0181] さらに、制御部102Cは、証明用訪問情報をユーザ端末20Cへ出力する旨を示す出力指示情報をカードリーダ30Cより受け取ると、一時的に記憶している端末IDに対応する証明用訪問情報を証明用訪問情報テーブルT300より取得し、取得した証明用歩門情報を入出力部103Cを介してカードリーダ30Cへ出力する。

(4) 入出力部103C

入出力部103Cは、第3の実施の形態にて示した認証カード10Bの入出力部103

Bと同様であるため、説明は省略する。つまり、入出力部103Cは、第1の実施の形態にて示した認証カード10の入出力部103、及び第2の実施の形態にて示した認証カード10Aの入出力部103Aとも同様である。

[0182] 4．4 ユーザ端末20Cの構成

ここでは、ユーザ端末20Cの構成について説明する。ユーザ端末20Cは、図24に示すように、認証鍵記憶部201C、認証部202C、表示部203C、入出力部204C、受信部205C、訪問情報記憶部206C及び時計部207Cとから構成されている。

[0183] ユーザ端末20Cは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Cは、その機能を達成する。

[0184] また、上記の身元認証システム1Cの概要にて示したように、ユーザ端末21C、・・・、22Cは、ユーザ端末20Cと同様の構成であるため、説明は省略する。

なお、ユーザ端末20Cにおけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

（1） 認証鍵記憶部201C

認証鍵記憶部201Cは、第3の実施の形態にて示したユーザ端末20Bの認証鍵記憶部201Bと同様であるため、説明は省略する。

[0185] （2） 訪問情報記憶部206C

訪問情報記憶部206Cは、耐タンパ性を有しており、配信装置50Cより送信された認証用訪問情報及び認証用訪問鍵を記憶する領域を備えている。

（3） 受信部205C

受信部205Cは、配信装置50Cよりインターネットを介して、認証用訪問情報及び認証用訪問鍵を受信すると、受信した認証用訪問情報及び認証用訪問鍵を訪問情報記憶部206Cへ書き込む。

[0186] これにより、ユーザ端末20Cは、訪問業者による訪問に係る情報を事前に記憶することができる。

（4） 時計部207C

時計部207Cは、時刻を計時する。

（5） 認証部202C

認証部202Cは、乱数を記憶する乱数記憶領域250Cを有しており、さらに、ユーザ端末20Cの端末ID（ここでは、「T−ID1」）をも予め記憶している。

[0187] 認証部202Cは、カードリーダ30Cより入出力部204Cを介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダ30Cに認証カード10Cが挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Cへ書き込む。次に、認証部202Cは、第1乱数「N1」を生成し、生成した第1乱数「N1」を入出力部204Cを介してカードリーダ30Cへ出力し、生成した第1乱数「N1」を乱数記憶領域250Cに記憶する。

[0188] さらに、認証部202Cは、カードリーダ30Cより入出力部204Cを介して、第1暗号化情報Enc（SK1、N1）を受け取ると、認証鍵記憶部201Cにて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報を用いて、第1暗号化情報Enc（SK1、N1）の復号を行い、復号により得られた復号結果と、乱数記憶領域250Cにて記憶している第1乱数「N1」とが一致するか否かを判断する。

[0189] 復号結果と第1乱数「N1」とが一致しない場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが不正な認証カードであると認証し、認証結果として不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Cへ出力する。さらに、認証部202Cは、認証鍵記憶部201Cにて記憶している身元認証指紋情報及び乱数記憶領域250Cにて記憶している第1乱数「N1」の消去を行う。

[0190] 復号結果と第1乱数「N1」とが一致する場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが正当な認証カードであると認証、つまり挿入された認証カードが正当な認証カードであると決定し、予め記憶している端末IDを取得し、さらに、第2乱数「N2」を生成し、乱数記憶領域250Cに記憶している内容を第1乱数「N1」から生成した第2乱数「N2」へと更新する。次に、認証部202Cは、生成した第2乱数「N2」と取得した端末IDとを入出力部204Cを介してカードリーダ30Cへ出力する。さらに、認証部202Cは、カードリーダ30Cより入出力部204Cを介して、第2暗号

化情報Enc(V—key1、N2)を受け取ると、訪問情報記憶部206Cにて記憶している認証用訪問鍵を取得する。

[0191] 認証部202Cは、受け取った第2暗号化情報Enc(V—key1、N2)を、取得した認証用訪問鍵を用いて、第2暗号化情報Enc(V—key1、N2)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Cにて記憶している第2乱数「N2」とが一致するか否かを判断する。

一致しない場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Cへ出力し、乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する。

[0192] 一致する場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが記憶している証明用訪問鍵が正当な証明用訪問鍵であると認証、つまり正当な訪問鍵であると決定し、出力指示情報を生成し、生成した出力指示情報を入出力部204Cを介してカードリーダ30Cへ出力する。さらに、認証部202Cは、カードリーダ30Cより入出力部204Cを介して、証明用訪問情報を受け取ると、次の動作を行う。認証部202Cは、訪問情報記憶部206Cにて記憶している認証用訪問情報を取得する。次に、受け取った証明用訪問情報に含まれる証明用時間情報及び証明用内容情報と、取得した認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断を行う。

[0193] 少なくとも何れかが一致しない場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Cへ出力する。

それぞれが一致すると判断する場合には、カードリーダ30Cに挿入された認証カードが記憶している証明用訪問情報は正当な証明用訪問情報であると認証、つまり正当な証明用訪問情報であると決定し、時計部207Cより現在時刻を取得し、取得した現在時刻が認証用時間情報にて示される訪問時間帯の範囲であるか否かを判断する。訪問時間帯の範囲でないと判断する場合には、認証部202Cは、カードリーダ30Cに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を

生成し、生成した不正訪問者情報を表示部203Cへ出力し、訪問情報記憶部206Cにて記憶している認証用訪問情報及び認証用訪問鍵、及び乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する。

[0194] 訪問時間帯の範囲であると判断する場合には、認証部202Cは、正当訪問者情報を生成し、生成した正当訪問者情報を表示部203Cへ出力し、訪問情報記憶部206Cにて記憶している認証用訪問情報、及び乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する。

(6) 表示部203C

表示部203Cは、第3の実施の形態にて示したユーザ端末20Bの表示部203Bと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したユーザ端末20の表示部203、及び第2の実施の形態にて示したユーザ端末20Aの表示部203Aとも同様である。

[0195] (7) 入出力部204C

入出力部204Cは、第3の実施の形態にて示したユーザ端末20Bの入出力部204Bと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したユーザ端末20の入出力部204、及び第2の実施の形態にて示したユーザ端末20Aの入出力部204Aとも同様である。

[0196] 4.5 カードリーダ30C

カードリーダ30Cは、図24に示すように、カード読取部301C、入出力部302C、表示部303C及び指紋読取部310Cから構成されている。

カードリーダ30Cは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ30Cは、その機能を達成する。

[0197] なお、上記の身元認証システム1Cの概要にて示したように、カードリーダ31C、・・・、32Cは、カードリーダ30Cと同様の構成であるため、説明は省略する。

なお、カードリーダ30Cにおけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

（1） カード読取部301C

カード読取部301Cは、認証カード10Cが挿入されたことの検知を行う。カード読取部301Cは、認証カード10Cが挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部303Cへ出力する。次に、カード読取部301Cは、指紋読取部310Cより身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部310Cより受け取った身元認証指紋情報とを入出力部302Cを介してユーザ端末20Cへ出力する。

[0198] カード読取部301Cは、ユーザ端末20Cより入出力部302Cを介して、第1乱数「N1」を受け取ると、受け取った第1乱数「N1」を認証カード10Cへ出力する。カード読取部301Cは、認証カード10Cより第1暗号化情報Enc（SK1、N1）を受け取ると、受け取った第1暗号化情報Enc（SK1、N1）を入出力部302Cを介してユーザ端末20Cへ出力する。

[0199] カード読取部301Cは、入出力部302Cを介してユーザ端末20Cより端末IDと第2乱数「N2」とを受け取ると、受け取った端末IDと第2乱数「N2」とを認証カード10Cへ出力する。さらに、カード読取部301Cは、認証カード10Cより第2暗号化情報Enc（V−key1、N2）を受け取ると、受け取った第2暗号化情報Enc（V−key1、N2）を入出力部302Cを介してユーザ端末20Cへ出力する。

[0200] カード読取部301Cは、入出力部302Cを介してユーザ端末20Cより出力指示情報を受け取ると、受け取った出力指示情報を認証カード10Cへ出力する。さらに、カード読取部301Cは、認証カード10Cより証明用訪問情報を受け取ると、受け取った証明用訪問を入出力部302Cを介してユーザ端末20Cへ出力する。

（2） 表示部303C

表示部303Cは、第3の実施の形態で示したカードリーダ30Bの表示部303Bと同様であるため、説明は省略する。

[0201] （3） 指紋読取部310C

指紋読取部310Cは、第3の実施の形態で示したカードリーダ30Bの指紋読取部310Bと同様であるため、説明は省略する。

（4） 入出力部302C

入出力部302Cは、第3の実施の形態にて示したカードリーダ30Bの入出力部302Bと同様であるため、説明は省略する。つまり、第1の実施の形態にて示したカードリーダ30の入出力部302、及び第2の実施の形態にて示したカードリーダ30Aの入出力部302Aとも同様である。

[0202] 4．6 訪問情報配信処理の動作

ここでは、認証用訪問情報を事前に配信する訪問情報配信処理について、図25に示す流れ図を用いて、説明する。

配信装置50Cは、利用者の操作により、認証用訪問情報をユーザ端末20Cへ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると(ステップS600)、認証用訪問鍵及び証明用訪問鍵とを生成する(ステップS605)。次に、配信装置50Cは、生成した認証用訪問鍵と、ステップS600にて受け取った訪問時間帯及び訪問内容とを用いて認証用訪問情報を生成する(ステップS610)。配信装置50Cは、生成した認証用訪問情報及び認証用訪問鍵をユーザ端末20Cへ送信する(ステップS610)。ユーザ端末20Cは、配信装置50Cより認証用訪問情報及び認証用訪問鍵を受信すると(ステップS620)、受信した認証用訪問情報及び認証用訪問鍵を訪問情報記憶部206Cへ書き込む(ステップS625)。

[0203] 配信装置50Cは、さらに、ステップS600にて受け取った訪問時間帯及び訪問内容とを用いて証明用訪問情報を生成し(ステップS630)、生成した証明用訪問情報及びステップS605にて生成した証明用訪問鍵を認証カード10Cへ出力する(ステップS635)。

認証カード10Cは、証明用訪問情報を受け取ると、受け取った証明用訪問情報を訪問鍵記憶部105Cへ書き込む(ステップS640)。

[0204] 4．7 身元認証処理の動作

ここでは、カードリーダ30Cに挿入された認証カード10Cの認証を行う処理である身元認証処理の動作について、図26及び図27に示す流れ図を用いて、説明する。

カードリーダ30Cは、認証カード10Cが挿入されたことを検知すると(ステップS650)、要求情報を生成し、生成した要求情報を表示する(ステップS655)。次に、カードリーダ30Cは、訪問者より入力された指紋より身元認証指紋情報を生成し(ステップS

660)、さらに、検知情報を生成し(ステップS665)、ステップS660にて生成した身元認証指紋情報と、ステップS665にて生成した検知情報とをユーザ端末20Cへ出力する(ステップS670)。

[0205] ユーザ端末20Cは、カードリーダ30Cより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Cへ書き込む(ステップS675)。次に、ユーザ端末20Cは、第1乱数「N1」を生成し、生成した第1乱数「N1」をカードリーダ30Cへ出力し、さらに、生成した第1乱数「N1」を乱数記憶領域250Cに記憶する(ステップS680)。

[0206] カードリーダ30Cは、ユーザ端末20Cより第1乱数「N1」を受け取ると、受け取った第1乱数「N1」を認証カード10Cへ出力する(ステップS685)。

認証カード10Cは、カードリーダ30Cより第1乱数「N1」を受け取ると(ステップS690)、受け取った第1乱数「N1」を証明鍵記憶部101Cにて記憶している身元証明鍵を用いて暗号化して、第1暗号化情報を生成し、生成した第1暗号化情報をカードリーダ30Cへ出力する(ステップS695)。

[0207] カードリーダ30Cは、認証カード10Cより第1暗号化情報を受け取ると、受け取った第1暗号化情報をユーザ端末20Cへ出力する(ステップS700)。

ユーザ端末20Cは、カードリーダ30Cより第1暗号化情報を受け取ると、受け取った第1暗号化情報と認証鍵記憶部201Cにて記憶している身元認証指紋情報とを用いて、認証処理を行う(ステップS705)。

[0208] ユーザ端末20Cは、認証処理にて、カードリーダに挿入された認証カードが正当な認証カードであると判断すると、端末IDを取得し(ステップS710)、さらに、第2乱数「N2」を生成し、乱数記憶領域250Cに記憶している内容を第1乱数「N1」から生成した第2乱数「N2」へと更新する(ステップS715)。次に、ユーザ端末20Cは、取得した端末IDと生成した第2乱数「N2」とをカードリーダ30Cへ出力する(ステップS720)。

[0209] カードリーダ30Cは、ユーザ端末20Cより端末IDと第2乱数「N2」とを受け取ると、受け取った端末IDと第2乱数「N2」とを認証カード10Cへ出力する(ステップS725)。

認証カード10Cは、カードリーダ30Cより端末IDと第2乱数「N2」とを受け取ると(ス

テップS730)、受け取った端末IDに対応する証明用訪問鍵を証明用訪問鍵テーブルT310より取得する(ステップS735)。次に、認証カード10Cは、取得した証明用訪問鍵を用いて、第2乱数「N2」を暗号化して、第2暗号化情報を生成し、生成した第2暗号化情報をカードリーダ30Cへ出力する(ステップS740)。

[0210] カードリーダ30Cは、認証カード10Cより第2暗号化情報を受け取ると、受け取った第2暗号化情報をユーザ端末20Cへ出力する(ステップS745)。

ユーザ端末20Cは、カードリーダ30Cより第2暗号化情報を受け取ると、受け取った第2暗号化情報と訪問情報記憶部206Cにて記憶している認証用訪問情報に含まれる認証用訪問鍵とを用いて、訪問鍵認証処理を行う(ステップS750)。

[0211] ユーザ端末20Cは、訪問鍵認証証処理にて、認証カード10Cに記憶されている証明用訪問情報が正当であると判断すると、出力指示情報を生成し、生成した出力指示情報をカードリーダ30Cへ出力する(ステップS755)。

カードリーダ30Cは、ユーザ端末20Cより出力指示情報を受け取ると、受け取った出力指示情報を認証カードへ出力する(ステップS760)。

[0212] 認証カード10Cは、カードリーダ30Cより出力指示情報を受け取ると、証明用訪問情報を証明用訪問情報テーブルT300より取得し、取得した証明用訪問情報をカードリーダ30Cへ出力する(ステップS765)。

カードリーダ30Cは、認証カード10Cより証明用訪問情報を受け取ると、受け取った証明用訪問情報をユーザ端末20Cへ出力する(ステップS770)。

[0213] ユーザ端末20Cは、カードリーダ30Cより証明用訪問情報を受け取ると、受け取った証明用訪問情報と、訪問情報記憶部206Cにて記憶している認証用訪問情報とを用いて、訪問情報検証処理を行う(ステップS775)。

4.8 認証処理

図26にて示した身元認証処理のステップS705にて行われる認証処理について、図19にて示した認証処理との変更点を中心に説明する。

[0214] 先ず、ステップS515にて、肯定的に判断する場合(ステップS515における「YES」)、ステップS520以降は行わないで、図27に示すステップS710以降を行うように変更する。否定的に判断する場合は(ステップS515における「NO」)、図19に示す動

作と同様である。なお、図27にて示す認証処理では、図19に示す乱数及び暗号化情報を、第1乱数及び第1暗号化情報と読み替える。

[0215] 4．9 訪問鍵認証処理

ここでは、図27にて示した身元認証処理のステップS750にて行われる訪問鍵認証処理について、図28に示す流れ図を用いて説明する。

ユーザ端末20Cは、認証カード10Cよりカードリーダ30Cを介して、第2暗号化情報を受け取る(ステップS800)。次に、ユーザ端末20Cは、訪問情報記憶部206Cにて記憶している認証用訪問鍵を取得し(ステップS805)、取得した認証用訪問鍵を用いて、第2暗号化情報の復号を行い(ステップS810)、復号により得られた復号結果と、乱数記憶領域250Cにて記憶している第2乱数「N2」とが一致するか否かを判断する(ステップS815)。

[0216] 一致すると判断する場合には(ステップS815における「YES」)、図27にて示すステップS755以降を行う。

一致しないと判断する場合には(ステップS815における「NO」)、不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Cへ出力し、乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する(ステップS820)。

[0217] 4．10 訪問情報検証処理

ここでは、図27にて示した身元認証処理のステップS775にて行われる訪問情報検証処理について、図29に示す流れ図を用いて説明する。

ユーザ端末20Cは、認証カード10Cよりカードリーダ30Cを介して、証明用訪問情報を受け取る(ステップS850)。次に、ユーザ端末20Cは、訪問情報記憶部206Cにて記憶している認証用訪問情報を取得する(ステップS855)。

[0218] ユーザ端末20Cは、取得した認証用訪問情報に含まれる認証用時間情報と、受け取った証明用訪問情報に含まれる証明用時間情報とが一致するか否かの判断、つまり事前に受信した訪問時間帯と認証カード10Cに記憶されている訪問時間帯とが一致するか否かの判断をする(ステップS860)。

時間帯が一致すると判断する場合には(ステップS860における「YES」)、取得した認証用訪問情報に含まれる認証用内容情報と、受け取った証明用訪問情報に含ま

れる証明用内容情報とが一致するか否かの判断、つまり事前に受信した訪問内容と認証カード10Cに記憶されている訪問内容とが一致するか否かの判断をする(ステップS865)。

[0219] 訪問内容が一致すると判断する場合には(ステップS865における「YES」)、時計部207Cより現在の時刻を取得し(ステップS870)、取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であるか否かを判断する(ステップS875)。

取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であると判断する場合には(ステップS875における「YES」)、正当訪問者情報を生成し、生成した正当訪問者情報を表示し(ステップS880)、訪問情報記憶部206Cにて記憶している認証用訪問情報、認証用訪問鍵及び乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する(ステップS890)。

[0220] 時間帯が一致しないと判断する場合(ステップS860における「NO」)、訪問内容が一致しないと判断する場合(ステップS865における「NO」)、及び取得した現在時刻が認証用時間情報に示される時間帯の範囲内でないと判断する場合(ステップS875における「NO」)のうち何れかの場合には、不正訪問者情報を生成し、生成した不正訪問者情報を表示し、訪問情報記憶部206Cにて記憶している認証用訪問情報、認証用訪問鍵及び乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する(ステップS890)。

[0221] 5. 実施例のまとめ

以上、説明したように、本発明によれば、身元認証システムは、認証カードとユーザ端末との間で認証を行っている。そのため、従来のようにネットワーク接続されたサーバを用いて認証を行う必要がない。例えば、ユーザ端末とサーバとが通信できないため、訪問者の身分の確認ができなくなるという問題は生じなくなる。

[0222] また、認証を行う毎に、乱数を発生させているため、認証カードにて生成される暗号化情報は、認証を行う毎に異なる内容となる。そのため、通信経路盗聴による成りすまし攻撃に対する耐性が高くなる。

また、身元認証鍵を配信する場合には、利用者宅の訪問前に任意のタイミングで身元認証鍵を配信することができるため、身元認証鍵の配信によるネットワーク負荷

を避けることができる。つまり、複数の利用者宅へ身元認証鍵を配信する際に、分散させて配信することが可能となる。

[0223] 6. 変形例

上記に説明した第1、第2、第3及び第4の実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

6. 1 通信方法の変形例

ユーザ端末と認証カードとの通信方法は、上記第1、第2、第3及び第4の実施の形態にて示した通信方法に限定されない。他の通信方法を用いてもよい。

[0224] 例えば、図30にて示す身元認証システム1Dの構成であってもよい。

身元認証システム1Dについて、一例として、第1の実施の形態と異なる点を中心に以下に説明する。

(A) 身元認証システム1Dの概要

身元認証システム1Dは、認証カード10D、ユーザ端末20D、第1入出力装置60D及び認証カードの着脱可能な第2入出力装置70Dとから構成される。ここでは、身元認証システム1Dの概要について説明を認証カード10Dとユーザ端末20Dと第1入出力装置60Dと第2入出力装置70Dとを用いて行う。

[0225] ユーザ端末20Dは、利用者の宅内に配置されており、具体的には、インターホンの親機である。第1入出力装置60Dは、利用者の宅外(例えば、玄関先)に配置されており、具体的には、インターホンの子機であり、ユーザ端末20Dと第1入出力装置60Dとは、ケーブル40Dにて接続されている。ユーザ端末20Dは、受話器290Dを備え、インターホンの親機としての機能動作を行う。第1入出力装置60Dは、呼出ボタン690D、マイク691D及びスピーカー692Dを備えており、インターホンの子機としての機能動作を行う。例えば、訪問者は、第1入出力装置60Dの呼出ボタン690Dを押下して、宅内にいる利用者を呼び出し、利用者は、受話器290Dを用い、訪問者は、マイク691D及びスピーカー692Dを用いて、インターホン越しに会話を行う。

[0226] また、第1入出力装置60Dは、画像受取部601D及び表示部602Dを備え、第2入

出力装置70Dは、画像受取部702D及び表示部703Dを備え、第1入出力装置60D及び第2入出力装置70Dとの間のデータの入出力を行う。

身元認証システム1Dは、認証カード10Dが第2入出力装置70Dの装着口790Dに装着されると、第1入出力装置60Dと第2入出力装置70Dとの間にて情報の入出力を行うことにより、第1の実施の形態にて示した認証処理を行う。ここでは、第1入出力装置60Dと第2入出力装置70Dとの間における情報の入出力をQRコードからなる画像情報を用いて行う。画像情報のやりとりは、以下のようにして行う。ユーザ端末20Dが画像情報を受け取る場合には、第1入出力装置60Dの画像受取部601Dを用いて、第2入出力装置70Dの表示部703Dにて表示された画像情報を受け取る。また、認証カード10Dが画像情報を受け取る場合には、第2入出力装置70Dの画像受取部702Dを用いて、第1入出力装置60Dの表示部602Dにて表示された画像情報を受け取る。

[0227] (B) 認証カード10Dの構成

ここでは、認証カード10Dの構成について説明する。認証カード10Dは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10Dは、図31に示すように、証明鍵記憶部101D、制御部102D及び入出力部103Dから構成されている。

[0228] 認証カード10Dは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10Dは、その機能を達成する。

(a) 証明鍵記憶部101D、入出力部103D

証明鍵記憶部101D及び入出力部103Dは、それぞれ証明鍵記憶部101及び入出力部103と同様であるため、説明は省略する。

[0229] (b) 制御部102D

制御部102Dは、第2入出力装置70Dより入出力部103Dを介して、証明鍵IDを要求する旨のID要求情報を受け取ると、証明鍵記憶部101Dより証明鍵IDを取得する。制御部102Dは、取得した証明鍵IDを用いて、ID用QRコードを生成し、生成

したID用QRコードを入出力部103Dを介して第2入出力装置70Dへ出力する。

[0230] さらに、制御部102Dは、第2入出力装置70Dより乱数「N」を示す乱数用QRコードを受け取ると、受け取った乱数用QRコードより乱数「N」を生成する。次に、制御部102Dは、証明鍵記憶部101Dより身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、乱数用RQコードより生成した乱数「N」に対して暗号化を施し、暗号化情報Enc(SK1、N)を生成する。制御部102Dは、生成した暗号化情報を暗号化用QRコードを生成し、生成した暗号化用QRコードを入出力部103Dを介して第2入出力装置70Dへ出力する。

[0231] (C) 第2入出力装置70D

ここでは、第2入出力装置70Dの構成について説明する。第2入出力装置70Dは、図31に示すように、カード読取部701D、画像受取部702D及び表示部703Dから構成されている。

第2入出力装置70Dは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第2入出力装置70Dは、その機能を達成する。

[0232] (a) カード読取部701D

カード読取部701Dは、認証カード10Dが装着されたことの検知を行う。カード読取部701Dは、認証カード10Dが挿入されたことを検知すると、ID要求情報を生成し、生成したID要求情報を認証カード10Dへ出力する。次に、認証カード10DよりID用QRコードを受け取ると、受け取ったID用QRコードを表示部703Dへ出力する。

[0233] さらに、カード読取部701Dは、第1入出力装置60Dより画像受取部702Dを介して、乱数用QRコードを受け取ると、受け取った乱数用QRコードを認証カード10Dへ出力する。カード読取部701Dは、認証カード10Dより暗号化用QRコードを受け取ると、受け取った暗号化用QRコードを表示部703Dへ出力する。

(b) 画像受取部702D

画像受取部702Dは、例えばカメラであり、第1入出力装置60Dにて表示されている画像を撮像し、撮像した画像をカード読取部701Dへ出力する。

[0234] (c) 表示部703D

表示部703Dは、例えばディスプレイであり、カード読取部701Dより受け取った情報を表示する。

(D) ユーザ端末20Dの構成

ここでは、ユーザ端末20Dの構成について説明する。ユーザ端末20Dは、認証カード10Dの認証を行う。ユーザ端末20Dは、図32に示すように、認証鍵記憶部201D、認証部202D、表示部203D及び入出力部204Dから構成されている。

[0235] ユーザ端末20Dは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Dは、その機能を達成する。

[0236] なお、ユーザ端末20Dにおけるインターホンの親機としての機能については、公知であるため、親機としての構成図及び説明は省略する。

(a) 認証鍵記憶部201D、表示部203D

認証鍵記憶部201D及び表示部203Dは、それぞれ認証鍵記憶部201及び表示部203と同様であるため、説明は省略する。

[0237] (b) 認証部202D

認証部202Dは、乱数を記憶する乱数記憶領域250D及び証明鍵IDを記憶するID記憶領域251Dを有している。

認証部202Dは、第1入出力装置60Dより入出力部204Dを介して、ID用QRコードを受け取ると、受け取ったID用QRコードより証明鍵IDを生成し、生成した証明鍵IDをID記憶領域251Dに記憶する。次に、認証部202Dは、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Dに記憶する。また、生成した乱数「N」を用いて、乱数用QRコードを生成し、生成した乱数用QRコードを入出力部204Dを介して第1入出力装置60Dへ出力する。さらに、認証部202Dは、第1入出力装置60Dより入出力部204Dを介して、暗号化用QRコードを受け取ると、受け取った暗号化用QRコードを用いて暗号化情報Enc(SK1、N)を生成する。次に、ID記憶領域251D

にて記憶している証明鍵IDと一致する認証鍵IDと対応する身元認証鍵を認証鍵記憶部201Dより取得し、取得した身元認証鍵を用いて、暗号化情報Enc（SK1、N）の復号を行い、復号により得られた復号結果と、乱数記憶領域250Dにて記憶している乱数「N」とが一致するか否かを判断する。一致すると判断する場合には、認証部202Dは、第2入出力装置70Dに装着されている認証カードが正当な認証カードであると認証、つまり第2入出力装置70Dに装着されている認証カードが正当な認証カードであると決定し、正当訪問者情報を生成して、生成した正当訪問者情報を表示部203Dへ出力する。一致しないと判断する場合には、認証部202Dは、第2入出力装置70Dに装着されている認証カードが不正な認証カードであると認証し、不正訪問者情報を生成して、生成した不正訪問者情報を表示部203Dへ出力する。

[0238] さらに、認証部202Dは、乱数記憶領域250Dに記憶している乱数「N」の消去、及びID記憶領域251Dに記憶している証明鍵IDの消去を行う。

（c） 入出力部204D

入出力部204Dは、第1入出力装置60Dより受け取った情報を認証部202Dへ出力し、認証部202Dから受け取った情報を第1入出力装置60Dへ出力する。

[0239] （E） 第1入出力装置60D

ここでは、第1入出力装置60Dの構成について説明する。第1入出力装置60Dは、図32に示すように、画像受取部601D、表示部602D及び入出力部603Dから構成されている。

第1入出力装置60Dは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第1入出力装置60Dは、その機能を達成する。

[0240] なお、第1入出力装置60Dにおけるインターホンの子機としての機能については、公知であるため、子機としての構成図及び説明は省略する。

（a） 画像受取部601D

画像受取部601Dは、例えばカメラであり、第2入出力装置70Dにて表示されている画像を撮像し、撮像した画像を入出力部603Dを介してユーザ端末20Dへ出力す

る。

[0241] (b) 表示部602D

表示部602Dは、例えばディスプレイであり、入出力部603Dを介してユーザ端末20Dより受け取った情報を表示する。

(F) 身元認証処理の動作

身元認証処理の動作は、第1の実施の形態にて示した身元認証処理の動作との変更点のみを説明する。先ず、カードリーダ30にて行っていた動作を第1入出力装置60D及び第2入出力装置70Dにて行うことになる。第1入出力装置60Dと第2入出力装置70Dとの情報の受け渡しは、それぞれに備えられた画像受取部を用いて、相手側装置に表示されている情報を撮像する。

[0242] また、ユーザ端末20Dでは、認証カード10Dへ出力する情報をQRコード化して出力するように変更し、認証カード10Dより受け取る情報は、QRコード化されているためQRコードより元の情報を生成して取得するように変更する。

認証カード10Dにおいてもユーザ端末20Dと同様に、ユーザ端末20Dへ出力する情報をQRコード化して出力するように変更し、ユーザ端末20Dより受け取る情報は、QRコード化されているためQRコードより元の情報を生成して取得するように変更する。

[0243] (G) 認証処理の動作

認証処理の動作は、第1の実施の形態にて示した認証処理の動作との変更点のみを説明する。ステップS100を、認証カード10Dより暗号化用QRコードを受け取り、受け取った暗号化用QRコードから暗号化情報を生成し、取得するように変更する。

(H)他の実施例への適用

これまで、第1の実施の形態と異なる点を中心に身元認証システム1Dの説明を行ったが、身元認証システム1Dにて用いたQRコードによる情報の受け渡しは第2、第3及び第4の実施の変形例として適用できる。

[0244] つまり、身元認証システムは、訪問者は利用者宅へ訪問した際に受け渡しされる情報をQRコード化して、QRコード化した情報の受け渡しを行えばよい。

なお、第3の実施の変形例として適用する場合には、第2入出力装置に、指紋読取

部310Bと同様の指紋読取部を備えることで、実現できる。また、第4の実施の変形例として適用する場合にも、同様に第2入出力装置に、指紋読取部を備えることで、実現できる。

[0245] 6．2 認証方法の変形例

上記の各実施の形態では、秘密鍵暗号処理を用いたチャレンジレスポンス方式の認証を行ったが、ここでは、他の暗号処理を用いたチャレンジレスポンス方式の認証について説明する。

(1)公開鍵暗号処理を用いる場合

ここでは、各実施の形態ごとに、公開鍵暗号処理を用いた場合の変形例について説明する。

[0246] ＜第1の実施の形態の変形例＞

公開鍵暗号処理を用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。ここで、公開鍵暗号処理は、一例として、RSAである。RSAについては、公知であるため、説明は省略する。

認証カード10は、身元証明鍵「SK1」を秘密鍵として、証明鍵IDと対応付けて記憶している。

[0247] ユーザ端末20は、公開鍵である身元認証鍵と、身元認証鍵を識別する認証鍵IDとからなる組を複数記憶している。なお、以降では、身元証明鍵「SK1」に対応する公開鍵である身元認証鍵を「PK1」として説明を行う。

ユーザ端末20は、カードリーダ30より検知情報と証明鍵IDとを受け取ると、証明鍵IDと一致する認証鍵IDに対応付けられた身元認証鍵「PK1」を取得する。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250に記憶し、さらに、生成した乱数「N」を取得した身元認証鍵「PK1」を用いて暗号化を行い、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)をカードリーダ30を介して認証カード10へ出力する。

[0248] 認証カード10は、ユーザ端末20より暗号化情報Enc(PK1、N)を受け取ると、受け取った暗号化情報Enc(PK1、N)を、記憶している身元証明鍵「SK1」を用いて、復号を行い、復号にて得られた復号結果をカードリーダ30を介してユーザ端末20へ

出力する。

ユーザ端末20は、認証カード10より復号結果を受け取ると、受け取った復号結果と、記憶している乱数「N」とが一致するか否かを判断を行い、一致すると判断する場合には、カードリーダ30Aに挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダ30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末20は、乱数記憶領域250にて記憶している情報及びデータを消去する。

[0249] ＜第2の実施の形態の変形例＞

第2の実施の形態と異なる点を中心に説明する。認証カード10Aは、秘密鍵として身元証明鍵「SK1」を認証鍵記憶部201Aにて記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された公開鍵である身元認証鍵「PK1」を記憶している。認証時の動作について、以下に説明する。ユーザ端末20Aは、カードリーダ30Aより検知情報を受け取ると、身元認証鍵「PK1」を認証鍵記憶部201Aより取得する。次に、ユーザ端末20Aは、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Aに記憶し、さらに、生成した乱数「N」を取得した身元認証鍵「PK1」を用いて暗号化を行い、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)をカードリーダ30Aを介して認証カード10Aへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Aにて記憶している乱数「N」の消去及び認証鍵記憶部201Aにて記憶している身元認証鍵「PK1」の消去を行う。

[0250] ＜第3の実施の形態の変形例＞

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID暗号を用いる。なお、ここで用いるID暗号は、ID情報に基づく公開鍵暗号処理である。この場合の具体例を以下に説明する。なお、ここでは、ID情報を指紋模様の特徴点からなる情報とする。また、ID情報に基づく公開鍵暗号処理については、公知技術であるため、説明は省略する。なお、A. Shamir著による「Identity-Base

d cryptosystems and signature schemes.」(In Advances in Cryptology - CRYPTO'84, Springer-Verlag LNCS 196, 47-53, 1984.)にて、ID情報に基づく公開鍵暗号処理についての詳細な記述がある。

[0251] 身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「SK」を生成し、生成した身元証明鍵「SK」を認証カード10Bの証明鍵記憶部101Bへ書き込む。

[0252] カードリーダ30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末20Bへ出力する。

ユーザ端末20Bは、カードリーダ30Bより身元認証指紋情報と検知情報とを受け取り、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成し、生成した公開鍵「PK」を認証鍵記憶部201Bに記憶する。さらに、ユーザ端末20Bは、乱数「N」をも生成し、生成した乱数「N」を乱数記憶領域250Bに記憶し、さらに、生成した乱数「N」を生成した公開鍵「PK」を用いて、暗号化情報Enc(PK、N)を生成し、生成した暗号化情報Enc(PK、N)をカードリーダ30Bを介して認証カード10Bへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Bにて記憶している乱数「N」の消去を行う。

[0253] これにより、バイオメトリックス情報と公開鍵暗号処理とを用いた認証方法が実現できる。

＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお

、カードリーダ30Cに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

[0254] (2)認証を行う毎に異なる電子署名を用いる場合

ここでは、各実施の形態ごとに、認証を行う毎に異なる電子署名を用いた場合の変形例について説明する。

＜第1の実施の形態の変形例＞

認証を行う毎に異なる電子署名を用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。

[0255] 認証カード10は、身元証明鍵「SK1」を秘密鍵として、証明鍵IDと対応付けて記憶している。

ユーザ端末20は、認証鍵記憶部201にて、公開鍵である身元認証鍵と、身元認証鍵を識別する認証鍵IDとからなる組を複数記憶している。なお、以降では、身元証明鍵「SK1」に対応する公開鍵である身元認証鍵を「PK1」として説明を行う。

[0256] ユーザ端末20は、カードリーダ30より検知情報と証明鍵IDとを受け取ると、受け取った証明鍵IDをID記憶領域251に記憶する。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250に記憶し、さらに、生成した乱数「N」をカードリーダ30を介して認証カード10へ出力する。

認証カード10は、ユーザ端末20より乱数「N」を受け取ると、記憶している身元証明鍵「SK1」を用いて、受け取った乱数「N」の電子署名を生成し、生成した電子署名をカードリーダ30を介してユーザ端末20へ出力する。

[0257] ユーザ端末20は、認証カード10より電子署名を受け取ると、ID記憶領域251にて記憶している証明鍵IDと一致する認証鍵IDに対応付けられた身元認証鍵「PK1」を認証鍵記憶部201より取得し、取得した身元認証鍵「PK1」と、乱数「N」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダ30に挿入された認証カードが正当な認証カードであると認証し

、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダ30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末20は、乱数記憶領域250にて記憶している乱数「N」、及びID記憶領域251にて記憶している証明鍵IDをそれぞれ消去する。

[0258] ＜第2の実施の形態の変形例＞

第2の実施の形態と異なる点を中心に説明する。認証カード10Aは、秘密鍵である、訪問者に対応する身元証明鍵「SK1」を認証鍵記憶部201Aにて記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された公開鍵である身元認証鍵「PK1」を記憶している。認証時の動作について、以下に説明する。ユーザ端末20Aは、カードリーダ30Aより検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Aに記憶し、さらに、生成した乱数「N」をカードリーダ30Aを介して認証カード10Aへ出力する。

[0259] 次に、上記で示した動作と同様に、認証カード10Aでは、乱数「N」の電子署名を生成して、生成した電子署名をユーザ端末20Aへ出力し、ユーザ端末20Aでは、事前に配信されている身元認証鍵と乱数「N」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Aにて記憶している乱数「N」の消去及び認証鍵記憶部201Aにて記憶している身元認証鍵「PK1」の消去を行う。

[0260] ＜第3の実施の形態の変形例＞

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID署名を用いる。なお、ここで用いるID署名は、ID情報に基づく電子署名方式であり、ID情報は指紋模様の特徴点からなる情報とする。ID署名については、公知技術であるため、説明は省略する。なお、A. Shamir著による「Identity-Based cryptosystems and signature schemes.」(In Advances in Cryptology - CRYPTO'84, Springer-Verlag LNCS 196, 47-53, 1984.)にて、ID署名についての詳細な記述がある。

[0261] ID署名を用いた場合の具体例を以下に説明する。

身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「SK」を生成し、生成した身元証明鍵「SK」を認証カード10Bの証明鍵記憶部101Bへ書き込む。

[0262] カードリーダ30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末20Bへ出力する。

ユーザ端末20Bは、カードリーダ30Bより身元認証指紋情報と検知情報を受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む。次に、ユーザ端末20Bは、乱数「N」を生成し、生成した乱数「N」をカードリーダ30Bを介して認証カード10Bへ出力し、生成した乱数「N」を乱数記憶領域250Bに記憶する。

[0263] 認証カード10Bは、ユーザ端末20Bより乱数「N」を受け取ると、記憶している身元証明鍵「SK」を用いて、受け取った乱数「N」の電子署名を生成し、生成した電子署名をカードリーダ30Bを介してユーザ端末20Bへ出力する。

ユーザ端末20Bは、認証カード10Bより電子署名を受け取ると、認証鍵記憶部201Bにて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成する。生成した身元認証鍵「PK」と、乱数「N」とを用いて、受け取った電子署名の署名検証を行う。

[0264] 以降は、上記と同様の動作であるため、説明は省略する。

＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダ30Cに挿入された認証カードが正当な認証カードであると認証した場

合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

[0265] (3)固定の電子署名を用いる場合

ここでは、各実施の形態ごとに、固定の電子署名を用いた場合の変形例について説明する。

＜第1の実施の形態の変形例＞

固定の電子署名を用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。

[0266] 身元認証システム1は、さらに、認証カード10の着脱が可能なサーバ装置を備え、サーバ装置は、身元証明鍵として電子署名を生成する秘密鍵「SK」を証明鍵IDと対応付けて記憶している。認証カード10は、証明鍵IDと身元証明鍵とを記憶する代わりに、認証カード10を識別するため識別子「ID」を記憶している。

また、ユーザ端末20は、認証鍵IDと身元認証鍵とを記憶する代わりに、身元認証鍵として公開鍵「PK」を認証鍵IDと対応付けて認証鍵記憶部201にて記憶している。

[0267] サーバ装置は、認証カード10が装着されると、認証カード10に記憶されている識別子「ID」を取得し、記憶している秘密鍵「SK」を用いて、取得した識別子「ID」の電子署名を生成し、生成した電子署名と秘密鍵「SK」と対応する証明鍵IDとを認証カード10に書き込む。

カードリーダ30は、認証カード10が挿入されたことを検知すると、認証カード10にて記憶している電子署名と証明鍵IDと識別子「ID」とを読み出し、読み出した電子署名と証明鍵IDと識別子「ID」とをユーザ端末20へ出力する。

[0268] ユーザ端末20は、電子署名と証明鍵IDと識別子「ID」とを受け取ると、受け取った証明鍵IDと一致する認証鍵IDに対応する公開鍵「PK」を認証鍵記憶部201より取得し、取得した公開鍵「PK」と、受け取った識別子「ID」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダ30に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情

報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダ30に挿入された認証カードが正当な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

[0269] ＜第2の実施の形態の変形例＞

第2の実施の形態と異なる点を中心に説明する。身元認証システム1Aは、さらに、上記と同様の動作を行うサーバ装置を備える。配信装置50Aは、身元認証鍵を記憶及びユーザ端末20Aへ配信する代わりに、公開鍵「PK」を記憶、及びユーザ端末20Aへ配信する。認証カード10Aは、身元証明鍵を記憶する代わりに、認証カード10Aを識別するため識別子「ID」を記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された身元認証鍵を記憶する代わりに、事前に配信装置50Aより配信された公開鍵「PK」を記憶している。

[0270] なお、認証時の動作については、上記と同様の動作であるため、説明は省略する。また、配信装置50Aとサーバ装置とは、同一の装置であってもよい。

＜第3の実施の形態の変形例＞

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID署名を用いる。なお、ここで用いるID署名は、ID情報に基づく電子署名であり、ID情報は、指紋模様の特徴点からなる情報とする。この場合の具体例を以下に説明する。

[0271] 身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。認証カード10Bは、証明鍵IDと身元証明鍵とを記憶する代わりに、認証カード10Bを識別するため識別子「ID」を記憶している。

サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵「SK」を生成する。さらに、サーバ装置は、挿入された認証カード10Bに記憶されている識別子「ID」を取得し、生成した秘密鍵「SK」を用いて、取得した識別子「ID」の電子署名を生成

し、生成した電子署名を認証カード10Bに書き込む。

[0272] カードリーダ30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成する。さらに、認証カード10Bにて記憶している電子署名と識別子「ID」とを読み出し、読み出した電子署名と識別子「ID」と生成した身元認証指紋情報とをユーザ端末20Bへ出力する。

[0273] ユーザ端末20Bは、カードリーダ30Bより電子署名と識別子「ID」と身元認証指紋情報とを受け取ると、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成する。ユーザ端末20Bは、生成した公開鍵「PK」と、受け取った識別子「ID」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記で示した動作と同様であるため、説明は省略する。

[0274] ＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダ30Cに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

(4)秘密鍵と一方向性関数とを用いる場合

先ず、一方向性関数について、説明する。一方向性関数とは、秘密鍵を入力として与えると、入力された秘密鍵とは異なる秘密鍵を出力し、出力された秘密鍵から入力に用いられた秘密鍵は生成されない関数である。また、一方向性関数は、同じ入力値からは、常に同じ値を出力する。

[0275] ＜第1の実施の形態の変形例＞

秘密鍵と一方向性関数とを用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。

認証カード10は、身元証明鍵「SK1」に、一方向性関数「f__1」を施した証明用秘密鍵「f__(SK1)」を、証明鍵IDと対応付けて記憶している。

[0276] ユーザ端末20は、図33に示すように、鍵情報テーブルT500を備えている。鍵情報テーブルT500は、身元認証鍵と、身元認証鍵を識別する認証鍵IDと、一方向性

関数とからなる組を複数記憶している。身元認証鍵及び認証鍵IDは、第1の実施の形態と同様であるため、説明は省略する。一方向性関数は、対応する身元認証鍵から、認証カード10の認証に必要な認証用秘密鍵を生成する関数である。

[0277] ユーザ端末20は、カードリーダ30より検知情報と証明鍵IDとを受け取ると、証明鍵IDと一致する認証鍵IDに対応付けられた身元認証鍵と一方向性関数とを取得する。ユーザ端末20は、取得した身元認証鍵に、取得した一方向性関数を施して、認証用秘密鍵を生成し、生成した認証用秘密鍵を一時的に記憶する。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250に記憶し、さらに、生成した乱数「N」をカードリーダ30を介して認証カード10へ出力する。

[0278] 認証カード10は、ユーザ端末20より乱数「N」を受け取ると、受け取った乱数「N」を、記憶している証明用秘密鍵「f__1(SK1)」を用いて、暗号化を施し、暗号化情報Enc(f__1(SK1)、N)を生成する。認証カード10は、生成した暗号化情報Enc(f__1(SK1)、N)をカードリーダ30を介してユーザ端末20へ出力する。

[0279] ユーザ端末20は、認証カード10より暗号化情報Enc(f__1(SK1)、N)を受け取ると、一時的に記憶している認証用秘密鍵を用いて、受け取った暗号化情報Enc(f__1(SK1)、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250にて記憶している乱数「N」とが一致するか否かを判断する。

以降は、第1の実施の形態と同様であるため、説明は省略する。

[0280] なお、ユーザ端末20は、乱数を生成する前に、認証用秘密鍵を生成したが、これに限定されない。ユーザ端末20は、暗号化情報を受け取った後、認証用秘密鍵を生成してもよい。

＜第2の実施の形態の変形例＞

第2の実施の形態と異なる点を中心に説明する。認証カード10Aは、証明用秘密鍵「f__1(SK1)」を認証鍵記憶部201Aにて記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された秘密鍵と、一方向性関数とを記憶している。認証時の動作について、以下に説明する。ユーザ端末20Aは、カードリーダ30Aより検知情報を受け取ると、記憶している秘密鍵に、記憶している一方向性関数を施して、認証用秘密鍵を生成し、生成した秘密鍵を一時的に記憶する。次に、ユーザ端末

20は、乱数「N」を生成し、生成した乱数「N」を入出力部204Aを介してカードリーダ30Aへ出力し、生成した乱数「N」を乱数記憶領域250Aに記憶する。

[0281] 認証カード10Aは、ユーザ端末20Aより乱数「N」を受け取ると、受け取った乱数「N」を、記憶している証明用秘密鍵「f__1(SK1)」を用いて、暗号化を施し、暗号化情報Enc(f__1(SK1)、N)を生成する。認証カード10Aは、生成した暗号化情報Enc(f__1(SK1)、N)をカードリーダ30Aを介してユーザ端末20Aへ出力する。

[0282] ユーザ端末20Aは、カードリーダ30Aより暗号化情報Enc(f__1(SK1)、N)を受け取ると、記憶している認証用秘密鍵を用いて、暗号化情報Enc(f__1(SK1)、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Aにて記憶している乱数「N」とが一致するか否かを判断する。

以降は、第2の実施の形態と同様であるため、説明は省略する。

[0283] なお、ユーザ端末20Aは、乱数を生成する前に、認証用秘密鍵を生成したが、これに限定されない。ユーザ端末20Aは、暗号化情報を受け取った後、認証用秘密鍵を生成してもよい。

＜第3の実施の形態の変形例＞

第3の実施の形態と異なる点を中心に説明する。

[0284] 認証カード10Bは、訪問者に対応する身元証明指紋情報、つまり身元証明鍵「SK1」に、一方向性関数「f__1」を施した証明用秘密鍵「f__(SK1)」を、証明用秘密鍵の生成に用いた一方向性関数を識別する証明用関数ID(例えば、「ID__1」)と対応付けて記憶している。

また、ユーザ端末20Bは、図34に示すように、情報テーブルT600を備えている。情報テーブルT600は、一方向性関数と、一方向性関数を識別する認証用関数IDとからなる組を複数記憶している。一方向性関数は、認証カード10の認証に必要な認証用秘密鍵を生成する関数である。認証用関数IDは、一方向性関数を識別する識別子であり、証明用関数IDと同一である。これにより、証明用秘密鍵の生成に用いた一方向性関数と、情報テーブルにて記憶している一方向性関数との対応付けが可能となる。

[0285] カードリーダ30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表

示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末20Bへ出力する。

ユーザ端末20Bは、カードリーダ30Bより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む。次に、認証部202Bは、乱数「N」を生成し、生成した乱数「N」を入出力部204Bを介してカードリーダ30Bへ出力し、生成した乱数「N」を乱数記憶領域250Bに記憶する。

[0286] 認証カード10Bは、ユーザ端末20Bより乱数「N」を受け取ると、受け取った乱数「N」を、記憶している証明用秘密鍵「f__1(SK1)」を用いて、暗号化を施し、暗号化情報Enc(f__1(SK1)、N)を生成する。認証カード10は、生成した暗号化情報Enc(f__1(SK1)、N)と、証明鍵ID「ID__1」とをカードリーダ30を介してユーザ端末20へ出力する。

[0287] ユーザ端末20Bは、カードリーダ30Bより入出力部204Bを介して、暗号化情報Enc(SK1、N)と証明鍵IDとを受け取ると、証明鍵IDと一致する認証IDに対応付けられた一方向性関数を取得する。ユーザ端末20は、記憶している身元認証指紋情報に、取得した一方向性関数を施して、認証用秘密鍵を生成し、生成した認証用秘密鍵を用いて、受け取った暗号化情報Enc(f__1(SK1)、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Bにて記憶している乱数「N」とが一致するか否かを判断する。

[0288] 以降は、第3の実施の形態と同様であるため、説明は省略する。

なお、ユーザ端末20Bは、暗号化情報を受け取った後、認証用秘密鍵を生成したが、これに限定されない。ユーザ端末20Aは、乱数を生成する前に、証明鍵IDを認証カード10Bより取得して、取得した証明鍵IDと一致する認証鍵IDに対応する一方向性関数を用いて、認証用秘密鍵を生成してもよい。

[0289] ＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。

(5)公開鍵証明書を用いる場合

先ず、公開鍵証明書について、説明する。公開鍵証明書とは、例えば、訪問業者

にて生成した公開鍵が、正しい公開鍵であることを示すものであり、第3者による機関である認証局(Certificate Authority:以下、CA)により発行される。

[0290] 公開鍵証明書は、訪問業者が生成した公開鍵、公開鍵証明書のID、及びそれらに対するCAの署名である証明書用署名を含む。ここで、証明書用署名は、CAだけが保持する秘密鍵(SK__CA)を用いて、デジタル署名を施して生成された署名データである。デジタル署名の一例は、ハッシュ関数を使ったRSA(Rivest Shamir Adleman)を用いるデジタル署名である。

[0291] 以下に、公開鍵証明書を用いた身元認証システム1000について、説明する。

身元認証システム1000は、認証カード1010、ユーザ端末1020及びカードリーダ1030とから構成される。

(a)認証カード1010

ここでは、認証カード1010の構成について説明する。認証カード1010は、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード1010は、図35に示すように、秘密鍵記憶部1101、証明書記憶部1102、制御部1103及び入出力部1104から構成されている。

[0292] 認証カード1010は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード1010は、その機能を達成する。

(秘密鍵記憶部1101)

秘密鍵記憶部1101は、耐タンパ性を有しており、秘密鍵を1つ記憶している。ここで記憶されている秘密鍵は、認証カード1010自身の正当性を証明するための訪問業者固有の鍵であり、訪問業者にて安全に管理されている。

[0293] 以降の説明において、必要に応じて、秘密鍵として「SK1」を用いて説明する。

(証明書記憶部1102)

証明書記憶部1102は、秘密鍵記憶部1101にて記憶している秘密鍵「SK1」に対応する公開鍵「PK1」の正当性を示す公開鍵証明書を記憶している。

(制御部1103)

制御部1103は、カードリーダ1030より入出力部1104を介して、公開鍵証明を要求する旨の証明書要求情報を受け取ると、証明書記憶部1102より公開鍵証明書を取得し、取得した公開鍵証明を入出力部1104を介してカードリーダ1030へ出力する。

[0294] さらに、制御部1103は、ユーザ端末1020よりカードリーダ1030を介して、乱数「N」が、公開鍵「PK1」にて暗号化された暗号化情報Enc(PK1、N)を受け取ると、秘密鍵記憶部1101より秘密鍵「SK1」を取得し、取得した秘密鍵「SK1」を用いて、受け取った暗号化情報Enc(PK1、N)を復号する。制御部1103は、復号結果を入出力部1104を介してカードリーダ1030へ出力する。

[0295] (入出力部1104)

入出力部1104は、カードリーダ1030より受け取った情報を制御部1103へ出力し、制御部1103から受け取った情報をカードリーダ1030へ出力する。

(b)ユーザ端末1020の構成

ここでは、ユーザ端末1020の構成について説明する。ユーザ端末1020は、カードリーダ1030に挿入された認証カード1010の認証を行う。ユーザ端末1020は、図36に示すように、CA公開鍵記憶部1201、認証部1202、表示部1203及び入出力部1204から構成されている。

[0296] ユーザ端末1020は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末1020は、その機能を達成する。

[0297] (CA公開鍵記憶部1201)

CA公開鍵記憶部1201は、耐タンパ性を有しており、CAだけが保持する秘密鍵(SK__CA)に対応する公開鍵(PK__CA)を記憶している。

(認証部1202)

認証部1202は、乱数を記憶する乱数記憶領域1250及び公開鍵証明書を記憶する証明書記憶領域1251を有している。

[0298] 認証部1202は、カードリーダ1030より入出力部1204を介して、カードリーダ1030に認証カード1010が挿入されたことを検知した旨を示す検知情報と、認証カード1010にて記憶している公開鍵証明書とを受け取る。

認証部1202は、CA公開鍵記憶部1201から公開鍵「PK__CA」を読み出し、読み出した公開鍵「PK__CA」を用いて、受け取った公開鍵証明書に含まれる証明書用署名の署名検証を行う。署名検証により、受け取った公開鍵証明書が正当なものであると判断する場合には、受け取った公開鍵証明書を、証明書記憶領域1251へ記憶する。

[0299] 認証部1202は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域1250に記憶する。

認証部1202は、証明書記憶領域1251にて記憶している公開鍵証明書に含まれる公開鍵「PK1」を取得し、生成した乱数「N」を、取得した公開鍵「PK1」を用いて、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)を、入出力部1204を介してカードリーダ1030へ出力する。

[0300] さらに、認証部1202は、カードリーダ1030より入出力部1204を介して、暗号化情報Enc(SK1、N)の復号結果を受け取り、受け取った復号結果と、乱数記憶領域1250にて記憶している乱数「N」とが一致するか否かを判断する。

復号結果と乱数「N」とが一致する場合には、認証部1202は、カードリーダ1030に挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部1203へ出力する。復号結果と乱数「N」とが一致しない場合には、認証部1202は、カードリーダ1030に挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部1203へ出力する。さらに、認証部1202は、乱数記憶領域1250に記憶している乱数「N」の消去、及び証明書記憶領域1251に記憶している公開鍵証明書の消去を行う。

[0301] また、認証部1202は、受け取った公開鍵証明書が正当なものでないと判断する場合には、不正訪問者情報を生成し、生成した不正訪問者情報を表示部1203へ出力

し、動作を終了する。

（表示部1203）

表示部1203は、例えば、ディスプレイを備え、認証部1202より受け取った認証結果の情報を外部に対して表示する。

[0302] （入出力部1204）

入出力部1204は、カードリーダ1030より受け取った情報を認証部1202へ出力し、認証部1202から受け取った情報をカードリーダ1030へ出力する。

（c）カードリーダ1030

カードリーダ1030は、図36に示すように、カード読取部1301及び入出力部1302から構成されている。

[0303] カードリーダ1030は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ1030は、その機能を達成する。

（カード読取部1301）

カード読取部1301は、認証カード1010が挿入されたことの検知を行う。カード読取部1301は、認証カード1010が挿入されたことを検知すると、検知情報及び証明書要求情報を生成し、生成した証明書要求情報を認証カード1010へ出力する。次に、認証カード1010より公開鍵証明書を受け取ると、受け取った公開鍵証明書と、生成した検知情報とを入出力部1302を介してユーザ端末1020へ出力する。

[0304] さらに、カード読取部1301は、ユーザ端末1020より入出力部1302を介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード1010へ出力する。カード読取部1301は、認証カード1010より暗号化情報Enc（SK1、N）を受け取ると、受け取った暗号化情報Enc（SK1、N）を入出力部1302を介してユーザ端末1020へ出力する。

[0305] （入出力部1302）

入出力部1302は、ユーザ端末1020より受け取った情報をカード読取部1301へ出力し、カード読取部1301から受け取った情報をユーザ端末1020へ出力する。

(d)身元認証処理の動作

ここでは、認証カード1010がカードリーダ1030に挿入されてからユーザ端末1020にて認証を行うまでの処理である身元認証処理の動作について、図37に示す流れ図を用いて説明する。

[0306] カードリーダ1030は、認証カード1010が挿入されたことを検知すると(ステップS1000)、検知情報及び証明書D要求情報を生成し、生成した証明書要求情報を認証カード1010へ出力する(ステップS1005)。

認証カード1010は、カードリーダ1030より証明書要求情報を受け取ると、証明書記憶部1102にて記憶している公開鍵証明書を取得し、取得した公開鍵証明書をカードリーダ1030へ出力する(ステップS1010)。

[0307] カードリーダ1030は、認証カード1010より公開鍵証明書を受け取ると(ステップS1015)、受け取った公開鍵証明書と、ステップS1005にて生成した検知情報とをユーザ端末1020へ出力する(ステップS1020)。

ユーザ端末1020は、カードリーダ1030より公開鍵証明書と検知情報とを受け取ると、受け取った公開鍵証明書の正当性を検証するために検証処理を行う(ステップS1025)。次に、ユーザ端末1020は、受け取った公開鍵証明書が正当なものである場合には、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域1250に記憶する(ステップS1030)。ユーザ端末1020は、公開鍵証明書に含まれる公開鍵「PK1」を取得し(ステップS1035)、取得した公開鍵「PK1」を用いて、乱数「N」を暗号化して、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)を、カードリーダ1030へ出力する(ステップS1040)。

[0308] カードリーダ1030は、ユーザ端末1020より暗号化情報Enc(PK1、N)を受け取ると、受け取った暗号化情報Enc(PK1、N)を認証カード1010へ出力する(ステップS1045)。

認証カード1010は、カードリーダ1030より暗号化情報Enc(PK1、N)を受け取ると、受け取った暗号化情報Enc(PK1、N)を秘密鍵記憶部1101にて記憶している秘密鍵「SK1」を用いて復号し、復号結果をカードリーダ1030へ出力する(ステップS1050)。

[0309] カードリーダ1030は、認証カード1010より復号結果を受け取ると、受け取った復号結果をユーザ端末1020へ出力する(ステップS1055)。

ユーザ端末1020は、カードリーダ1030より復号結果を受け取ると、受け取った復号結果と、乱数記憶領域1250に記憶している乱数「N」とを用いて、認証処理を行う(ステップS1060)。

[0310] (e)検証処理

ここでは、身元認証処理のステップS1025にて行われる検証処理について、図38に示す流れ図を用いて説明する。

ユーザ端末1020の認証部1202は、カードリーダ1030より、検知情報と、認証カード1010にて記憶している公開鍵証明書とを受け取ると(ステップS1100)、CA公開鍵記憶部1201にて記憶しているCAの公開鍵(PK__CA)を取得する(ステップS1105)。

[0311] 認証部1202は、取得した公開鍵「PK__CA」を用いて、受け取った公開鍵証明書に含まれる証明書用署名の署名検証を行う(ステップS1110)。認証部1202は、署名検証により、受け取った公開鍵証明書が正当なものか否かを判断する(ステップS1115)。

正当なものであると判断する場合には(ステップS1115における「YES」)、認証部1202は、受け取った公開鍵証明書を、証明書記憶領域1251へ記憶し(ステップS1120)、図37に示すステップS1030以降を行う。

[0312] 正当なものでないと判断する場合には(ステップS1115における「NO」)、認証部1202は、不正訪問者情報を生成し、生成した不正訪問者情報を表示し(ステップS1125)、処理を終了する。

(f)認証処理

ここでは、身元認証処理のステップS1060にて行われる認証処理について、図39に示す流れ図を用いて説明する。

[0313] ユーザ端末1020の認証部1202は、認証カード1010よりカードリーダ1030を介して暗号化情報の復号結果を受け取る(ステップS1200)

認証部1202は、受け取った復号結果と、乱数記憶領域1250にて記憶している乱

数「N」とが一致するか否かの判断を行う(ステップS1205)。

一致すると判断する場合には(ステップS1205における「YES」)、正当訪問者情報を生成し、生成した正当訪問者情報を表示し(ステップS1210)、乱数記憶領域1250に記憶している乱数「N」、及び証明書記憶領域1251に記憶している公開鍵証明書をそれぞれ消去し(ステップS1220)、処理を終了する。

[0314] 一致しないと判断する場合には(ステップS1205における「NO」)、不正訪問者情報を生成し、生成した不正訪問者情報を表示し(ステップS1215)、乱数記憶領域1250に記憶している乱数「N」、及び証明書記憶領域1251に記憶している公開鍵証明書をそれぞれ消去し(ステップS1220)、処理を終了する。

6.3 身元認証システム1000の変形例

上記に説明した身元認証システム1000は、本発明の実施の一例であり、本発明はこの身元認証システム1000に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

[0315] (1)上記の身元認証システム1000のユーザ端末1020において、CAの公開鍵「PK__CA」を予め記憶していたが、第2の実施の形態と同様に、配信装置を設けて、訪問前に、配信装置からユーザ端末1020へCAの公開鍵を配信してもよい。

(2)上記の身元認証システム1000のユーザ端末1020は、第4の実施の形態と同様に、訪問鍵による認証及び、訪問情報の検証を行ってもよい。または、訪問鍵による認証のみを行ってもよいし、訪問情報による検証のみを行ってもよい。

[0316] 6.4 認証後の動作の変形例

上記の各実施の形態では、認証結果をユーザ端末に表示したが、これに限定されない。

例えば、認証が成功した場合には、ユーザ端末は、訪問者の名前及び顔写真を表示してもよいし、または、物品の送り主の名前、物品名及びメッセージを表示してもよい。

(a)訪問者の名前及び顔写真を表示する場合

ここでは、訪問者の名前及び顔写真を表示する場合の変形例について、第1の実

施の形態を用いて、説明する。

[0317] 認証カード10は、上記第1実施の形態にて示す構成に加えて、訪問者の名前及び顔写真のデータとからなる訪問者情報を記憶している訪問者情報記憶部を有している。

認証カード10は、暗号化情報を、ユーザ端末20へ出力する際に、訪問者情報記憶部に記憶している訪問者情報を出力する。

ユーザ端末20の認証部202は、暗号化情報と訪問者情報とを、認証カード10から受け取ると、受け取った訪問者情報を一時的に記憶し、受け取った暗号化情報を用いて、認証を行う。

[0318] 認証部202は、認証処理による認証が成功すると、正当訪問者情報を生成する代わりに、一時的に記憶している訪問者情報を取得し、取得した訪問者情報に含まれる顔写真のデータに基づいて、顔写真の画像を生成し、生成した画像と、受け取った訪問者情報に含まれる訪問者の名前とを、表示部203へ出力する。表示部203は、認証部202より顔写真の画像と、名前とを受け取ると、受け取った画像及び名前を表示する。

[0319] なお、訪問者の名前及び顔写真の表示は、他の実施の形態においても適用できる。各実施の形態における認証カードに、さらに、上記と同様の訪問者情報記憶部を設けて、上記と同様の動作を行うことで、実現することができる。

また、上記の変形例にて示す身元認証システム1000においても、上記と同様の訪問者情報記憶部を設けて、上記と同様の動作を行うことで、実現することができる。

[0320] なお、認証成功時に表示する内容は、訪問者の名前のみであってもよいし、訪問者の顔写真の画像のみであってもよい。

また、認証カード10は、訪問者情報を、暗号化情報を出力する際に、ユーザ端末20へ出力したが、これに限定されない。例えば、ユーザ端末20において、認証が成功した場合に、認証カード10は、訪問者情報を、ユーザ端末20へ出力してもよい。

[0321] このとき、ユーザ端末20は、認証が成功すると、訪問者情報を要求する要求情報を、カードリーダ30を介して認証カード10へ出力し、認証カード10は、要求情報を受け取ると、訪問者情報を訪問者情報記憶部より取得し、取得した訪問者情報を、カー

ドリーダ30を介してユーザ端末20へ出力する。

これにより、認証成功後に、表示された訪問者の名前や顔写真の画像を表示することで、ユーザは、玄関ドアののぞき穴から、訪問者の顔の確認や、訪問者の名札に記載した名前の確認することができ、さらに安全性を高めることができる。

[0322] (b)物品の送り主の名前、物品名及びメッセージを表示する場合

ここでは、送り主の名前、物品名及びメッセージを表示する場合の変形例について、第1の実施の形態を用いて、説明する。

認証カード10は、上記第1実施の形態にて示す構成に加えて、送り主の名前、物品名及び送り主からのメッセージとからなる送り主情報を記憶している送り主情報記憶部を有している。

[0323] 認証カード10は、暗号化情報を、ユーザ端末20へ出力する際に、送り主情報記憶部に記憶している送り主情報を出力する。

ユーザ端末20の認証部202は、暗号化情報と送り主情報とを、認証カード10から受け取ると、受け取った送り主情報を一時的に記憶し、受け取った暗号化情報を用いて、認証を行う。

[0324] 認証部202は、認証処理による認証が成功すると、正当訪問者情報を生成する代わりに、一時的に記憶している送り主情報を取得し、取得した送り主情報に含まれる送り主の名前、物品名及びメッセージを、表示部203へ出力する。表示部203は、認証部202より送り主の名前、物品名及びメッセージを表示する。

なお、物品の送り主の名前、物品名及びメッセージの表示は、他の実施の形態においても適用できる。各実施の形態における認証カードに、さらに、上記と同様の送り主情報記憶部を設けて、上記と同様の動作を行うことで、実現することができる。

[0325] また、上記の変形例にて示す身元認証システム1000においても、上記と同様の送り主情報記憶部を設けて、上記と同様の動作を行うことで、実現することができる。

なお、認証成功時に表示する内容は、送り主の名前のみであってもよいし、物品名のみであってもよいし、メッセージのみであってもよい。または、これらのうち2つからなる情報であってもよい。

[0326] また、認証カード10は、送り主情報を、暗号化情報を出力する際に、ユーザ端末2

0へ出力したが、これに限定されない。例えば、ユーザ端末20において、認証が成功した場合に、認証カード10は、送り主情報を、ユーザ端末20へ出力してもよい。

このとき、ユーザ端末20は、認証が成功すると、送り主情報を要求する要求情報を、カードリーダ30を介して認証カード10へ出力し、認証カード10は、要求情報を受け取ると、送り主情報を送り主情報記憶部より取得し、取得した送り主情報を、カードリーダ30を介してユーザ端末20へ出力する。

[0327] これにより、届いた物品が、見知らぬ者からのものであるか否かの確認ができる。

なお、物品の送り主の名前、物品名及びメッセージの表示に加えて、上記にて示す訪問者の名前及び顔写真の表示を行ってもよい。

このとき、認証カード10にて、訪問者情報記憶部及び送り主情報記憶部を備えることにより、実現することができる。

[0328] 6．5 その他の変形例

上記に説明した各実施の形態及び各変形例は、本発明の実施の一例であり、本発明は各実施の形態及び各変形例に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

(1)上記各実施の形態及び各変形例において、認証方法をチャレンジレスポンス方式としたが、これに限定されない。他の認証方法を用いてもよい。

[0329] 例えば、一方向性の認証である。この場合の認証方法について、第1の実施の形態に基づいて、以下に説明する。

認証カード10は、カードリーダ30に挿入されると、乱数「N」を生成し、記憶している身元証明鍵「SK1」を用いて、生成した乱数「N」を暗号化し、暗号化情報Enc(SK1、N)を生成する。次に、認証カード10は、生成した乱数「N」と暗号化情報Enc(SK1、N)とをカードリーダ30を介してユーザ端末20へ出力する。

[0330] ユーザ端末20は、認証カード10より乱数「N」と暗号化情報Enc(SK1、N)とを受け取ると、記憶している身元認証鍵「SK1」を用いて、受け取った暗号化情報Enc(SK1、N)を復号する。ユーザ端末20は、復号して得られた復号結果と認証カード10より受け取った乱数「N」とが一致するか否かを判断し、一致すると判断する場合には

、カードリーダ30に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダ30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

[0331] また、第2の実施の形態においては、認証カード10Aは、上記にて示した動作と同様の動作を行う。ユーザ端末20Aは、認証カード10Aより受け取った乱数「N」と暗号化情報Enc(SK1、N)と、配信装置50Aより事前に受け取り、記憶している身元認証鍵とを用いて、上記にて示した動作と同様の動作を行う。なお、認証後は、事前に記憶している身元認証鍵を消去する。

[0332] また、第3の実施の形態においては、認証カード10Bは、上記にて示した動作と同様の動作を行う。ユーザ端末20Bは、認証カード10Bより受け取った乱数「N」と暗号化情報Enc(SK1、N)と、カードリーダ30Bより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

また、第4の実施の形態においては、認証カード10Cは、上記にて示した動作と同様の動作を行う。ユーザ端末20Cは、認証カード10Cより受け取った乱数「N」と暗号化情報Enc(SK1、N)と、カードリーダ30Cより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

[0333] (2)上記各実施の形態及び各変形例において、認証カードをカードリーダへ挿入して、認証を行ったが、これに限定されない。

カードリーダの表面にセンサー部を設け、認証カードをセンサー部へ接触させることにより認証を行ってもよい。

または、認証カードに無線タグを備え付け、センサー部とは非接触とすることによる認証を行ってもよい。

[0334] (3)上記各実施の形態及び各変形例において、ユーザ端末とカードリーダとをケーブルにて接続したが、これに限定されない。

ユーザ端末とカードリーダとを無線による通信にて接続してもよい。

(4)上記各実施の形態において、認証結果をユーザ端末に表示したが、これに限定されない。

[0335] 認証により、正当な訪問者であると判断する場合には、玄関のドアの鍵を解除するようにしてもよい。この場合、玄関のドアは電子ロックにて鍵の施錠及び解除を行う。鍵の施錠及び解除を行う構成部を玄関制御部と呼ぶ。ユーザ端末は、カードリーダに挿入された認証カードが正当な認証カードであると認証した場合には、正当訪問者情報を生成し、生成した正当訪問者情報を玄関制御部に出力し、カードリーダに挿入された認証カードが不正な認証カードであると認証した場合には、不正訪問者情報を生成し、生成した不正訪問者情報を玄関制御部へ出力する。玄関制御部は、ユーザ端末より受け取った情報が正当訪問者情報及び不正訪問者情報のうち何れかであるかを判断し、正当訪問者情報であると判断する場合には、鍵の解除を行い、不正訪問者情報であると判断する場合には、鍵の解除を行わない。

[0336] または、ユーザ端末に玄関ドアの施錠を解除する解除ボタンを設けてもよい。この場合、認証が成功し、解除ボタンを押下すると、玄関ドアの施錠が解除され、認証が失敗した場合、解除ボタンを押下しても玄関ドアは解除されない。例えば、子供が留守番している場合には、子供が、誤って解除ボタンを押下することが考えられるが、その場合においても、認証に成功しない限りは、玄関ドアは解除されないという優れた効果を発揮する。

[0337] または、認証結果を、予め指定した固定電話機や携帯電話機に認証結果を通知してもよい。通知方法は、例えば、自動メッセージや電子メールである。

(5)上記通信方法の変形例では、QRコードを用いたが、他の画像情報であってもよい。例えば、バーコードである。

また、画像情報以外のものであってもよい。例えば、光信号である。

[0338] (6)上記通信方法の変形例では、情報の受け渡しを、ディスプレイによる表示とカメラによる画像の撮像により行ったが、これに限定されない。

例えば、第1及び第2入出力装置に赤外線機能を設けて、赤外線通信による情報の受け渡しを行ってもよい。このとき通信に用いられる信号は赤外線信号である。

または、第1及び第2入出力装置にスピーカとマイクとを設けて、受け渡しを行う情報を音声信号に変換して、変換した音声信号による通信を行ってもよい。

[0339] (7)上記通信報穂の変形例において、情報の受け渡しに第1及び第2入出力装置

を用いたが、これに限定されない。

例えば、第1入出力装置が有する機能をユーザ端末に設けて、第2入出力装置を認証カードの着脱が可能なカメラ付携帯電話機としてもよい。このとき、情報の受け渡しは、玄関ののぞき穴を利用して行われる。

[0340] (8)上記通信方法の変形例において、ユーザ端末20Dから認証カード10Dへ情報を出力する方法と、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報を出力する方法を同一の方法としたが、これに限定されない。ユーザ端末20Dから認証カード10Dへ情報を出力する方法と、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報を出力する方法とをそれぞれ異なる方法としてもよい。

[0341] 例えば、ユーザ端末20Dから認証カード10Dへ情報を出力する方法としてQRコードを用い、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報出力する方法として、音声信号を用いる。

(9)上記各実施の形態及び各変形例において、ユーザ端末から認証カードへ出力する情報、認証カード及びカードリーダからユーザ端末へ出力する情報をそれぞれ他の情報に変換して出力してもよい。

[0342] 例えば、ユーザ端末から認証カードへ出力する情報をQRコード化して、認証カードへ出力してもよい。このとき、認証カードは、ユーザ端末よりカードリーダを介してQRコード化された情報を受け取ると、受け取ったQRコード化された情報を用いて、元の情報を生成することになる。また、同様に、認証カード及びカードリーダからユーザ端末へ出力する情報をQRコード化して、ユーザ端末へ出力してもよい。このとき、ユーザ端末は、認証カードよりカードリーダを介してQRコード化された情報やカードリーダよりQRコード化された情報を受け取ると、受け取ったQRコード化された情報を用いて、元の情報を生成することになる。

[0343] なお、上記に例では、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダから情報を出力する方法とを同一の方法(QRコード化した情報を出力する方法)としたが、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダから情報を出力する方法とをそれぞれ異なる方法としてもよい。

例えば、ユーザ端末から情報を出力する方法としてQRコードを用いて、認証カード及びカードリーダから情報を出力する方法として音声信号を用いる。

[0344] (10)上記各実施の形態及び各変形例において、認証カードに制御部を設けたが、これに限定されない。認証カードに制御部を設けないで、カードリーダに制御部を設けて、認証カード内で行っていた処理をカードリーダにて行ってもよい。

また、上記通信方法の変形例においても同様に、認証カードに制御部を設けないで、第2入出力装置に制御部を設けて、認証カード内で行っていた処理を第2入出力装置にて行ってもよい。

[0345] (11)上記各実施の形態及び各変形例において、ユーザ端末を携帯電話機としてもよい。このとき、携帯電話機は、認証部を予め備えておいてもよいし、認証部と同様の動作を行うアプリケーションを訪問業者が有するアプリケーション配信装置よりダウンロードすることにより入手して、記憶してもよい。

または、ユーザ端末をインターホンの代わりにテレビドアホンとしてもよい。

[0346] (12)上記各実施の形態及び各変形例において、認証カードがユーザ端末を識別するようにしてもよい。

このとき、ユーザ端末は、端末IDを予め記憶しており、認証カードは、端末IDを記憶する記憶領域を備えている。ユーザ端末は、認証後、正当な訪問者であると判断する場合に、予め記憶している端末IDを認証カードへ出力する。認証カードは、受け取った端末IDを記憶領域へ記憶する。

[0347] これにより、記憶領域に記憶された端末IDを訪問履歴として利用することができる。

(13)上記各実施の形態及び各変形例において、認証カードが、ユーザ端末を認証するようにしてもよい。

これにより、配達証明と同様のことが実現できる。

(14)上記第1の実施の形態において、ユーザ端末20に記憶している身元認証鍵の変更及びユーザ端末20へ身元認証鍵の追加を行ってもよい。

[0348] このとき、身元認証システム1は、さらに、配信装置を備え、配信装置は、ユーザ端末20へ、認証IDと身元認証鍵とからなる組を送信する。ユーザ端末20は、配信装置より、認証IDと身元認証鍵とからなる組を受信すると、受信した認証IDと一致する

認証IDが鍵情報テーブルT100に存在するか否かを判断する。存在すると判断する場合には、受信した認証IDと一致する認証IDに対応する身元認証鍵を受信した身元認証鍵へと書き替える。存在しないと判断する場合には、新規の身元認証鍵として、受信した認証IDと身元認証鍵とからなる組を鍵情報テーブルT100に追加する。

[0349] （15）上記第2の実施の形態において、身元認証鍵を配信する場合には、配信する身元認証鍵を暗号化して配信してもよい。このとき、ユーザ端末は、暗号化された身元認証鍵を復号する復号鍵を、耐タンパ性を有する記憶領域にて予め記憶しており、受信した暗号化された身元認証鍵を復号鍵にて復号を行い、復号された身元認証鍵を、耐タンパ性を有する認証鍵記憶部にて記憶する。

[0350] （16）第2の実施の形態では、配信装置50Aとユーザ端末20Aをネットワーク接続する際にインターネットを利用したが、これに限定されない。専用線によるネットワーク接続であってもよい。

（17）第2の実施の形態において、配信装置50Aより事前に配信され、記憶している身元認証鍵を認証後、消去したが、これに限定されない。

[0351] 認証後も、消去しないで記憶しておいてもよい。このとき、ユーザ端末20Aは、配信装置50Aより身元認証鍵を受け取ると、受け取った身元認証鍵と記憶している身元認証鍵とが一致するか否かを判断し、一致すると判断する場合には、鍵の書き換えは行わず、一致しないと判断する場合には、記憶している身元認証鍵から受け取った身元認証鍵へと書き換えを行う。

[0352] （18）上記第3の実施の形態において、認証に用いるバイオメトリックス情報として指紋模様の特徴点からなる情報（以下、単に「指紋情報」という。）を用いたが、これに限定されない。

バイオメトリックス情報として、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のDNAの特徴を示すDNA情報又は、これら情報の組合せである。

[0353] このとき、声紋情報を用いる場合は、カードリーダ30Bには、訪問者の音声を受け取り、受け取った音声から訪問者の声紋の特徴を示す身元認証声紋情報を生成する声紋読取部を設け、認証カード10Bには、訪問者の声紋の特徴を示す身元証明

声紋情報を予め記憶しておく。

また、虹彩情報を用いる場合は、カードリーダ30Bには、訪問者の虹彩を読み取り、読み取った虹彩から訪問者の虹彩の特徴を示す身元認証虹彩情報を生成する虹彩読取部を設け、認証カード10Bには、訪問者の虹彩の特徴を示す身元証明虹彩情報を予め記憶しておく。

[0354] また、輪郭情報を用いる場合は、カードリーダ30Bには、訪問者の顔の輪郭を読み取り、読み取った顔の輪郭から訪問者の顔の輪郭の特徴を示す身元認証輪郭情報を生成する輪郭読取部を設け、認証カード10Bには、訪問者の顔の輪郭の特徴を示す身元証明輪郭情報を予め記憶しておく。

また、DNA情報を用いる場合は、カードリーダ30Bには、訪問者のDNAを解析したDNA情報である身元認証DNA情報を受け付けるDNA情報読取部を設け、認証カードには、訪問者のDNAを解析したDNA情報である身元証明DNA情報を予め記憶しておく。ここで、DNA情報とは、例えば、訪問者の髪の毛、血液又は唾液より解析される情報である。

[0355] なお、第4の実施の形態においても同様に、バイオメトリックス情報を、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のDNAの特徴を示すDNA情報又は、これら情報の組合せとしてもよい。

(19)上記第3及び第4の実施の形態において、カードリーダよりユーザ端末へ出力する身元認証指紋情報を暗号化して出力してもよい。

[0356] このとき、カードリーダは、身元認証指紋情報を暗号化する暗号鍵を予め記憶しており、また、ユーザ端末は、受け取った暗号化された身元認証指紋情報を復号する復号鍵を予め記憶することで実現できる。

(20)上記第4の実施の形態にて示した訪問鍵認証処理において、チャレンジレスポンス方式による認証方法として、秘密鍵暗号処理を用いたが、これに限定されない。上記認証方法の変形例と同様に、他の暗号処理を用いたチャレンジレスポンス方式による認証方法でもよいし、上記(1)と同様に他の認証方法でもよい。

[0357] (21)上記認証方法の変形例(a)において、公開鍵をユーザ端末、秘密鍵を認証

カードへそれぞれ記憶したが、これに限定されない。

公開鍵を認証カード、秘密鍵をユーザ端末へそれぞれ記憶してもよい。このときの認証の動作は、秘密鍵暗号処理を用いた場合と同様であるため、説明は省略する。

(22)上記各実施の形態及び各変形例において、身元認証システムの構成要件であるユーザ端末とカードリーダとをそれぞれ個別の装置として扱ったが、これに限定されない。

[0358] ユーザ端末とカードリーダとをユーザ端末とカードリーダとからなる1つの装置して扱ってもよい。

また、上記通信方法の変形例においても同様に、ユーザ端末と第1入出力装置とからなる1つの装置として扱ってもよい。

(23)第4の実施の形態において、証明用訪問鍵と認証用訪問鍵とを基に認証を行う場合、第2乱数を生成して認証に使用したが、これに限定されない。第2乱数を生成しないで、先の認証にて使用した第1乱数を用いて、証明用訪問鍵と認証用訪問鍵とを基に認証を行ってもよい。このとき、図26及び図27にて示した身元認証処理においては、ステップS715を乱数記憶領域250Cにて記憶している第1乱数「N1」をカードリーダ30Cへ出力するように変更し、以下の動作にて第2乱数「N2」を用いる代わりに、第1乱数「N1」を用いて動作するように変更すればよい。

[0359] (24)第4の実施の形態において、認証用訪問鍵と証明用訪問鍵とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時間帯の判断を行ったが、これに限定されない。

認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時間帯の判断を行ってもよい。

[0360] または、認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致

するか否かの判断のみ行ってもよいし、訪問時間帯の判断のみ行ってもよい。

または、身元認証指紋情報と身元証明情報とを基にした認証後に、認証用訪問鍵と証明用訪問鍵とを基にした認証のみを行ってもよい。

[0361] (25)上記第1、第2及び第3の実施の形態において、認証カードの証明鍵記憶部のみが耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

例えば、上記第1の実施の形態において、認証カード10の構成要素である証明鍵記憶部101、制御部102及び入出力部103の全てが耐タンパ性を有してもよい。

また、第4の実施の形態においても同様に、認証カードの証明鍵記憶部及び訪問鍵記憶部が耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

[0362] (26)上記各実施の形態及び各変形例において、ユーザ端末は、認証カードより受け取った暗号化情報(第4の実施の形態では、第1暗号化情報)を復号し、復号して得られた復号結果と、生成し記憶している乱数(第4の実施の形態では、第1乱数)とを用いて、復号結果と乱数(第4の実施の形態では、第1乱数)とが一致するか否かの判断を行ったが、これに限定されない。

[0363] ユーザ端末は、生成し記憶している乱数(第4の実施の形態では、第1乱数)を、記憶している身元認証鍵(第3及び第4の実施の形態では、身元認証指紋情報)を用いて暗号化して、暗号化乱数を生成し、生成した暗号化乱数と、認証カードより受け取った暗号化情報とを用いて、暗号化乱数と暗号化情報とが一致するか否かの判断を行い、一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

[0364] (27)上記各実施の形態及び各変形例において、ユーザ端末は、生成した乱数(第4の実施の形態では、第1乱数)を認証カードへ出力したが、身元認証鍵(第3及び第4の実施の形態では、身元認証指紋情報)を用いて、乱数を暗号化して暗号化乱数を生成し、生成した暗号化乱数を出力してもよい。

このとき、認証カードでは、ユーザ端末より受け取った暗号化乱数を、身元証明鍵

を用いて復号して得られた復号結果をユーザ端末へ出力し、ユーザ端末では、認証カードより受け取った復号結果と、記憶している乱数(第4の実施の形態では、第1乱数)とが一致するか否かの判断を行う。一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

[0365] (28)上記第4の実施の形態の認証カード10Cにおいて、証明用訪問情報テーブルT300にて記憶する証明用時間情報及び証明用内容情報、つまり証明用訪問情報は、暗号化して記憶してもよい。

このとき、配信装置50Cは、証明用訪問情報を暗号化する暗号鍵を記憶しており、証明用訪問情報を認証カード10Cに記録する際に、記憶している暗号化鍵を用いて暗号化して、記録する。また、ユーザ端末20Cは、配信装置50Cが記憶している暗号化鍵に対応する復号鍵を記憶しており、訪問情報検証処理を行う際に、暗号化された証明用訪問情報を、認証カード10Cより取得して、取得した暗号化された証明用訪問情報を、記憶している復号鍵を用いて復号して、証明用訪問情報を生成して、生成した証明用訪問情報を用いて、訪問情報検証処理を実行する。

[0366] (29)宅配業者による訪問は、アパートメントの一室であってもよい。このとき、カードリーダが設けられる玄関は、各アパートメントの部屋のドアであってもよいし、アパートメント全体の出入り口であるエントランスに設けられたドアであってもよい。

(30)カードリーダが施錠を検出するドアは、宅配物を収納する宅外に設けられた収納ボックスのドアであってもよい。

[0367] (31)本発明の対象は、宅配物の配送先であれば、一般の家に限らず、会社等のビジネスユーザでもよい。

(32)施錠状態の検知は、第2、第3及び第4の実施の形態に適用してもよいし、上記に示す各変形例に適用してもよい。

(33)第1の実施の形態において、カードリーダ30は、施錠されている状態を検出しない場合に、施錠メッセージを表示したが、警告音にて、ユーザに施錠を促してもよい。

[0368] または、カードリーダ30は、施錠されている状態を検出しない場合には、電子的な制御により、ドアを施錠してもよい。

(34)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0369] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD—ROM、MO、DVD、DVD—ROM、DVD—RAM、BD(Blu—ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0370] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0371] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(35)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0372] 上記において説明した身元認証システムは、訪問業者による訪問者が利用者宅に訪問して、セールス、宅配サービス、その他サービスの提供などを行う産業において、経営的、つまり反復的かつ継続的に利用されうる。

請求の範囲

[1] 宅配業者が有する可搬型の記録媒体と、前記宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者による訪問の正当性を認証する認証装置と、前記記録媒体と前記認証装置との間における情報の入出力を行い、玄関先に設けられた入出力装置とからなる認証システムであって、

前記記録媒体は、

前記宅配業者による訪問の正当性に係る情報を、少なくとも1つ予め記憶しており、

前記認証装置は、

前記宅配業者による訪問の正当性の検証に係る情報を、少なくとも1つ記憶しており、前記入出力装置を介して、前記記録媒体に記憶されている前記情報と、当該装置にて記憶している前記情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する

ことを特徴とする認証システム。

[2] 前記記録媒体は、ICカードであり、

前記入出力装置は、前記ICカードのカードリーダであり、

前記カードリーダは、さらに、玄関ドアの施錠状態を検出し、

前記認証装置は、前記カードリーダにて玄関ドアが施錠されている状態が検出された場合に、前記認証を行う

ことを特徴とする請求項1に記載の認証システム。

[3] 前記ICカードは、前記宅配業者による訪問の正当性に係る情報として、前記宅配業者の正当性を証明する証明情報を記憶しており、

前記認証装置は、前記宅配業者による訪問の正当性の検証に係る情報として、前記証明情報を検証するための認証情報を記憶しており、

前記認証装置は、前記証明情報と記憶している前記認証情報とを用いて、前記カードリーダを介して、前記宅配業者による訪問が正当であるか否かの認証を行う

ことを特徴とする請求項2に記載の認証システム。

[4] 前記ICカードは、前記宅配業者による訪問の正当性に係る情報として、さらに、前

記宅配業者による訪問の内容を示す第1訪問情報を予め記憶しており、

前記認証装置は、前記宅配業者による訪問の正当性の検証に係る情報として、さらに、前記第1訪問情報にて示される情報を検証するための第2訪問情報を記憶しており、

前記認証装置は、前記証明情報と前記認証情報とを用いた認証の結果が肯定的である場合に、前記ICカードより前記カードリーダを介して、前記第1訪問情報を取得し、取得した前記第1訪問情報と、記憶している前記第2訪問情報とが一致するか否かを判断し、判断結果が肯定的である場合に、前記宅配業者による訪問が正当であると判断する

ことを特徴とする請求項3に記載の認証システム。

[5] 前記第1訪問情報は、宅配業者による訪問の時間帯を示す第1時間情報であり、

前記第2訪問情報は、宅配業者にて訪問を受ける時間帯を示す第2時間情報であり、

前記認証装置は、前記第1時間情報と前記第2時間情報とが一致するか否かを判断する

ことを特徴とする請求項4に記載の認証システム。

[6] 前記第1訪問情報は、宅配業者の訪問内容を示す第1訪問内容情報であり、

前記第2訪問情報は、宅配業者にて訪問を受ける内容を示す第2訪問内容情報であり、

前記認証装置は、前記第1訪問内容情報と前記第2訪問内容情報とが一致するか否かを判断する

ことを特徴とする請求項4に記載の認証システム。

[7] 前記第1訪問情報は、宅配業者による訪問の時間帯を示す第1時間情報と、宅配業者の訪問内容を示す第1訪問内容情報とを含み、

前記第2訪問情報は、宅配業者にて訪問を受ける時間帯を示す第2時間情報と、宅配業者にて訪問を受ける内容を示す第2訪問内容情報とを含み、

前記認証装置は、前記第1時間情報と前記第2時間情報とが一致するか否か、及び前記第1訪問内容情報と前記第2訪問内容情報とが一致するか否かを判断する

ことを特徴とする請求項4に記載の認証システム。

[8] 前記ICカードは、さらに、前記宅配業者にて届けられた物品に係る物品情報を記憶しており、

前記認証装置は、さらに、前記ICカードより前記カードリーダを介して、前記物品情報を取得し、前記宅配業者による訪問が正当であると判断する場合に、前記物品情報を表示する

ことを特徴とする請求項4に記載の認証システム。

[9] 前記物品情報は、送り主の名前であり、

前記認証装置は、前記ICカードより送り主の名前を取得し、取得した名前を表示する

ことを特徴とする請求項8に記載の認証システム。

[10] 前記物品情報は、前記物品の物品名であり、

前記認証装置は、前記ICカードより前記物品の物品名を取得し、取得した物品名を表示する

ことを特徴とする請求項8に記載の認証システム。

[11] 前記物品情報は、送り主からのメッセージであり、

前記認証装置は、前記ICカードより送り主からのメッセージを取得し、取得したメッセージを表示する

ことを特徴とする請求項8に記載の認証システム。

[12] 前記ICカードは、訪問者を識別する訪問者情報を記憶しており、

前記認証装置は、さらに、前記ICカードより前記カードリーダを介して、前記訪問者情報を取得し、前記宅配業者による訪問が正当であると判断する場合に、前記訪問者情報を表示する

ことを特徴とする請求項4に記載の認証システム。

[13] 前記訪問者情報は、訪問者の名前であり、

前記認証装置は、前記ICカードより訪問者の名前を取得し、取得した名前を表示する

ことを特徴とする請求項12に記載の認証システム。

[14] 前記訪問者情報は、訪問者の顔写真の画像であり、

前記認証装置は、前記ICカードより前記訪問者の顔写真の画像を取得し、取得した顔写真の画像を表示する

ことを特徴とする請求項12に記載の認証システム。

[15] 前記訪問者情報は、訪問者の名前、及び顔写真の画像であり、

前記認証装置は、前記ICカードより前記訪問者の名前、及び顔写真の画像を取得し、取得した名前、及び顔写真の画像を表示する

ことを特徴とする請求項12に記載の認証システム。

[16] 前記認証装置及び前記ICカードは、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行う

ことを特徴とする請求項4に記載の認証システム。

[17] 前記証明情報は、暗号化鍵であり、

前記認証情報は、復号鍵であり、

前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記暗号化鍵を用いて暗号化して、レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、

前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記復号データを用いて前記レスポンスを復号して、復号データを生成して、生成した復号データと、前記チャレンジデータとが一致するか否かの認証を行う

ことを特徴とする請求項16に記載の認証システム。

[18] 前記暗号化鍵は、前記ICカードの所有者の生体科学的特徴を示す所有者証明情報であり、

前記認証装置は、さらに、

訪問者の生体科学的特徴を示す所有者認証情報を受け付け、受け付けた所有者認証情報を、前記復号鍵とする

ことを特徴とする請求項17に記載の認証システム。

[19] 前記認証装置は、さらに、前記復号鍵を配信する配信装置とネットワークを介して接続されており、

前記認証装置は、さらに、

前記宅配業者の訪問を受ける前に、前記配信装置から配信される前記復号鍵を受信し、受信した前記復号鍵を記憶する

ことを特徴とする請求項17に記載の認証システム。

[20] 前記認証情報は、秘密鍵であり、

前記ICカードは、前記秘密鍵と同一の鍵に対して、一方向性関数が施された第1鍵を記憶しており、

前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記第1鍵を用いて暗号化して、レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、

前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記秘密鍵に、前記前記一方向性関数と同一の処理を行う関数を施して第2鍵を生成し、生成した前記第2鍵を用いて、前記レスポンスを復号して、復号データを生成して、生成した復号データと、前記チャレンジデータとが一致するか否かの認証を行う

ことを特徴とする請求項16に記載の認証システム。

[21] 前記認証情報は、第1秘密鍵であり、

前記ICカードは、前記第1秘密鍵と同一の内容である第2秘密鍵を記憶しており、

前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、受け取った前記チャレンジデータを、前記第2秘密鍵を用いて暗号化して、レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装

置へ出力し、

前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記第1秘密鍵を用いて前記チャレンジデータを暗号化して、暗号化データを生成し、生成した前記暗号化データと、前記レスポンスデータとが一致するか否かの認証を行う

ことを特徴とする請求項16に記載の認証システム。

[22] 前記証明情報は、秘密鍵であり、

前記認証情報は、前記秘密鍵に対応する公開鍵であり、

前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置より前記チャレンジデータを受け取り、前記秘密鍵を用いて、受け取った前記チャレンジデータの電子署名を生成し、生成した電子署名を前記レスポンスデータとして、前記カードリーダを介して前記認証装置へ出力し、

前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、前記公開鍵と前記チャレンジデータとを用いて、前記チャレンジデータの署名検証による認証を行う

ことを特徴とする請求項16に記載の認証システム。

[23] 前記秘密鍵は、前記ICカードの所有者の生体科学的特徴を示す所有者証明情報であり、

前記認証装置は、さらに、

訪問者の生体科学的特徴を示す所有者認証情報を受け付け、受け付けた所有者認証情報を、前記公開鍵とする

ことを特徴とする請求項22に記載の認証システム。

[24] 前記証明情報は、秘密鍵であり、

前記認証情報は、前記秘密鍵に対応する公開鍵であり、

前記認証装置は、チャレンジデータを生成し、生成したチャレンジデータを、前記公開鍵を用いて暗号化し、前記暗号化されたチャレンジデータを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置より前記暗号化されたチャレンジデータを受け取り、前記秘密鍵を用いて、受け取った前記暗号化されたチャレンジデータを復号して、前記レスポンスデータを生成して、生成した前記レスポンスデータを、前記カードリーダを介して前記認証装置へ出力し、

前記認証装置は、前記ICカードより前記レスポンスデータを受け取ると、受け取った前記レスポンスデータと、前記チャレンジデータとが一致するか否かの認証を行う

ことを特徴とする請求項16に記載の認証システム。

[25] 前記ICカードは、前記公開鍵を含み、且つ前記公開鍵の正当性を証明する公開鍵証明書を記憶しており、

前記認証装置は、さらに、

前記公開鍵証明書を、前記ICカードから取得し、取得した前記公開鍵証明書の正当性を検証し、検証結果が肯定的である場合に、前記公開鍵証明書に含まれる前記公開鍵を、記憶する

ことを特徴とする請求項24に記載の認証システム。

[26] 前記ICカードは、宅配業者が訪問前に前記認証装置へに配布した第1訪問鍵と同一の第2訪問鍵を記憶しており、

前記認証装置は、さらに、前記第1訪問鍵を記憶しており、

前記認証装置は、

チャレンジレスポンスによる認証の結果が肯定的である場合に、さらに、第1訪問検証データを生成し、生成した前記訪問検証データを、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記訪問検証データを受け取ると、前記第2訪問鍵を用いて、受け取った前記訪問検証データを暗号化し、前記暗号化された訪問検証データを、前記カードリーダを介して前記認証装置へ出力し、

前記認証装置は、前記第1訪問鍵を用いて、受け取った暗号化された訪問検証データを復号して、復号結果と、前記訪問検証データとが一致するか否かを判断し、一致する場合に、第1訪問情報と第2訪問情報とが一致するか否かを判断する

ことを特徴とする請求項16に記載の認証システム。

[27] 前記認証装置は、前記ICカードへ前記チャレンジデータを出力する際に、前記チャレンジデータのデータ構造とは異なるデータ構造からなり、且つ前記チャレンジデータと同一の内容を示す変換チャレンジ情報へと変換し、前記変換チャレンジ情報を前記チャレンジデータとして前記ICカードへ出力する

ことを特徴とする請求項16に記載の認証システム。

[28] 前記ICカードは、前記認証装置へ前記レスポンスデータを出力する際に、前記レスポンスデータのデータ構造とは異なるデータ構造からなり、且つ前記レスポンスデータと同一の内容を示す変換レスポンス情報へと変換し、前記変換レスポンス情報を前記レスポンスデータとして前記認証装置へ出力する

ことを特徴とする請求項27に記載の認証システム。

[29] 前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなり、

前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる

ことを特徴とする請求項28に記載の認証システム。

[30] 前記認証装置は、さらに、自己を識別する装置識別子を記憶しており、

前記認証装置は、前記宅配業者による訪問が正当であると判断する場合に、前記装置識別子を、前記カードリーダを介して前記ICカードへ出力し、

前記ICカードは、前記認証装置から前記装置識別子を受け取ると、受け取った前記装置識別子を記憶する

ことを特徴とする請求項16に記載の認証システム。

[31] 宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者が有する可搬型の記録媒体を用いて、前記宅配業者の訪問の正当性を認証する認証装置であって、

前記認証の処理に用いる情報を記憶している情報記憶手段と、

玄関先に設けられた入出力装置を介して、前記記録媒体が記憶している前記訪問業者による訪問の正当性に係る情報と、前記情報記憶手段にて記憶している情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する判断手段と

を備えることを特徴とする認証装置。

[32] 前記入出力装置は、前記記録媒体のカードリーダであり、

前記カードリーダは、玄関ドアの施錠状態を検出し、

前記判断手段は、前記カードリーダにて玄関ドアが施錠されている状態が検出された場合に、前記認証を行う

ことを特徴とする請求項31に記載の認証装置。

[33] 前記記録媒体は、前記宅配業者による訪問の正当性に係る情報として、前記宅配業者の正当性を証明する証明情報を記憶しており、

前記情報記憶手段は、前記認証の処理に用いる情報として、前記宅配業者の正当性を検証する認証情報を記憶しており、

前記判断手段は、前記証明情報と記憶している前記認証情報とを用いて、前記カードリーダを介して、前記宅配業者による訪問が正当であるか否かの認証を行う

ことを特徴とする請求項32に記載の認証装置。

[34] 前記記録媒体は、前記宅配業者による訪問の正当性に係る情報として、さらに、前記宅配業者による訪問の内容を示す第1訪問情報を予め記憶しており、

前記情報記憶手段は、さらに、前記第1訪問情報にて示される情報を検証するための第2訪問情報を記憶しており、

前記判断手段は、前記証明情報と前記認証情報とを用いた認証の結果が肯定的である場合に、前記記録媒体より前記カードリーダを介して、前記第1訪問情報を取得し、取得した前記第1訪問情報と、記憶している前記第2訪問情報とが一致するか否かを判断し、判断結果が肯定的である場合に、前記宅配業者による訪問が正当であると判断する

ことを特徴とする請求項33に記載の認証装置。

[35] 前記記録媒体は、さらに、前記宅配業者にて届けられた物品に係る物品情報を記憶しており、

前記認証装置は、さらに、前記記録媒体より前記カードリーダを介して、前記物品情報を取得する物品情報取得手段と、

前記判断手段による判断の結果が肯定的である場合に、前記物品情報を表示す

る物品情報表示手段と

を備えることを特徴とする請求項34に記載の認証装置。

[36] 前記記録媒体は、訪問者を識別する訪問者情報を記憶しており、

前記認証装置は、さらに、前記記録媒体より前記カードリーダを介して、前記訪問者情報を取得する訪問者情報取得手段と、

前記判断手段による判断の結果が肯定的である場合に、前記訪問者情報を表示する訪問者情報表示手段と

を備えることを特徴とする請求項34に記載の認証装置。

[37] 前記認証装置及び前記記録媒体は、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行う

ことを特徴とする請求項34に記載の認証装置。

[38] 前記認証装置は、携帯電話機である

ことを特徴とする請求項37に記載の認証装置。

[39] 宅配業者が有し、前記宅配業者の訪問を受ける者の家屋内に設けられ、前記宅配業者による正当性を認証する認証装置に用いられる可搬型の記録媒体であって、

前記宅配業者による訪問の正当性に係る情報を、少なくとも1つ予め記憶している記憶手段と、

前記認証装置から玄関先に設けられた入出力装置を介して、第1データを受け取る受取手段と、

前記記憶手段にて記憶している情報を用いて、認証の処理に用いられる第2データを、前記第1データより生成するデータ生成手段と、

生成した前記第2データを、前記入出力装置を介して前記認証装置へ出力する出力手段と

を備えることを特徴とする記録媒体。

[40] 前記記憶手段は、前記宅配業者による訪問の正当性に係る情報として、前記宅配業者の正当性を証明する証明情報を記憶しており、

前記データ生成手段は、前記証明情報を用いて、前記第2データを生成する

ことを特徴とする請求項39に記載の記録媒体。

[41] 前記記憶手段は、前記宅配業者による訪問の正当性に係る情報として、さらに、前記宅配業者による訪問の内容を示す訪問情報を予め記憶しており、

前記出力手段は、さらに、前記訪問情報を、前記入出力装置を介して前記認証装置へ出力する

ことを特徴とする請求項40に記載の記録媒体。

[42] 前記記録媒体は、さらに、

前記宅配業者にて届けられた物品に係る物品情報を記憶している物品情報記憶手段を備え、

前記出力手段は、さらに、前記物品情報を、前記入出力装置を介して前記認証装置へ出力する

ことを特徴とする請求項41に記載の記録媒体。

[43] 前記記録媒体は、さらに、

訪問者を識別する訪問者情報を記憶している訪問者情報記憶手段を備え、

前記出力手段は、さらに、前記訪問者情報を、前記入出力装置を介して前記認証装置へ出力する

ことを特徴とする請求項41に記載の記録媒体。

[44] 前記認証装置は、前記証明情報の正当性を認証する認証情報を記憶しており、

前記認証装置及び前記記録媒体は、前記証明情報と前記認証情報とを用いて、チャレンジレスポンス型の認証処理を行う

ことを特徴とする請求項41に記載の記録媒体。

[45] 前記記録媒体は、携帯電話機に装着される

ことを特徴とする請求項44に記載の記録媒体。

[46] 宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者が有する可搬型の記録媒体を用いて、前記宅配業者の訪問の正当性を認証する認証装置に用いられる認証方法であって、

前記認証装置は、

前記認証の処理に用いる情報を記憶している情報記憶手段を備え、

前記認証方法は、

玄関先に設けられた入出力装置を介して、前記記録媒体が記憶している前記訪問業者による訪問の正当性に係る情報と、前記情報記憶手段にて記憶している情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する判断ステップと

を含むことを特徴とする認証方法。

[47] 宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者が有する可搬型の記録媒体を用いて、前記宅配業者の訪問の正当性を認証する認証装置に実行させる認証プログラムであって、

前記認証装置は、

前記認証の処理に用いる情報を記憶している情報記憶手段を備え、

前記認証プログラムは、

玄関先に設けられた入出力装置を介して、前記記録媒体が記憶している前記訪問業者による訪問の正当性に係る情報と、前記情報記憶手段にて記憶している情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する判断ステップと

を含むことを特徴とする認証プログラム。

[48] 宅配業者の訪問を受ける者が家屋内にて有し、前記宅配業者が有する可搬型の記録媒体を用いて、前記宅配業者の訪問の正当性を認証する認証装置に実行させる認証プログラムを記録したコンピュータ読み取り可能なプログラム記録媒体であって、

前記認証装置は、

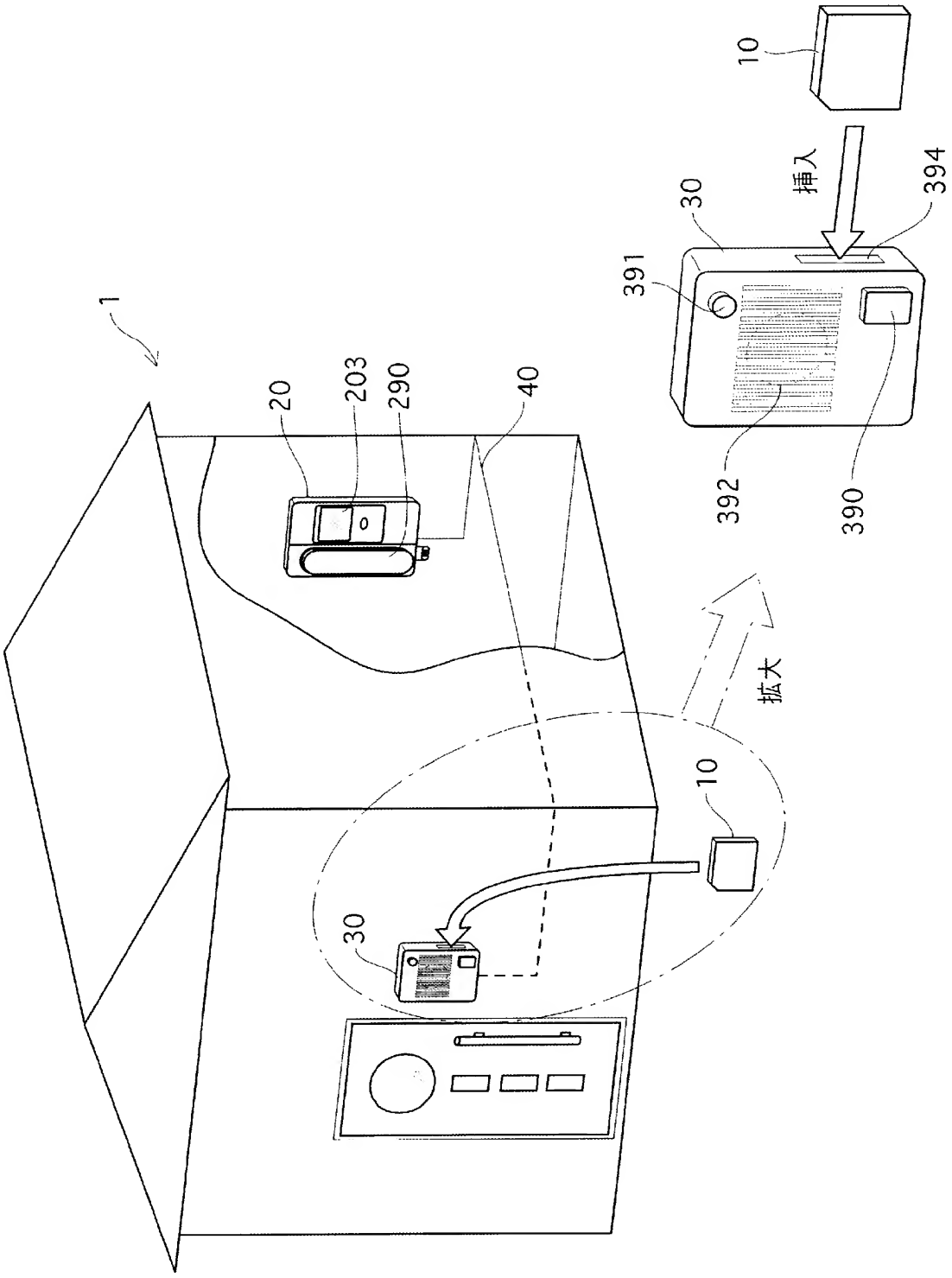
前記認証の処理に用いる情報を記憶している情報記憶手段を備え、

前記認証プログラムは、

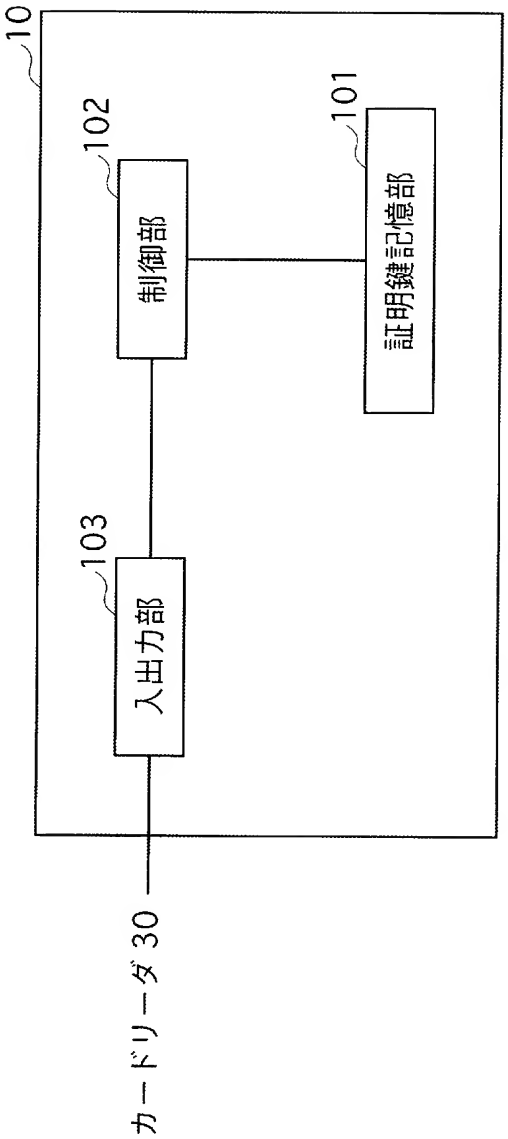
玄関先に設けられた入出力装置を介して、前記記録媒体が記憶している前記訪問業者による訪問の正当性に係る情報と、前記情報記憶手段にて記憶している情報とを用いた認証を行い、前記記録媒体を有する前記宅配業者による訪問が正当であるか否かを判断する判断ステップと

を含むことを特徴とするプログラム記録媒体。

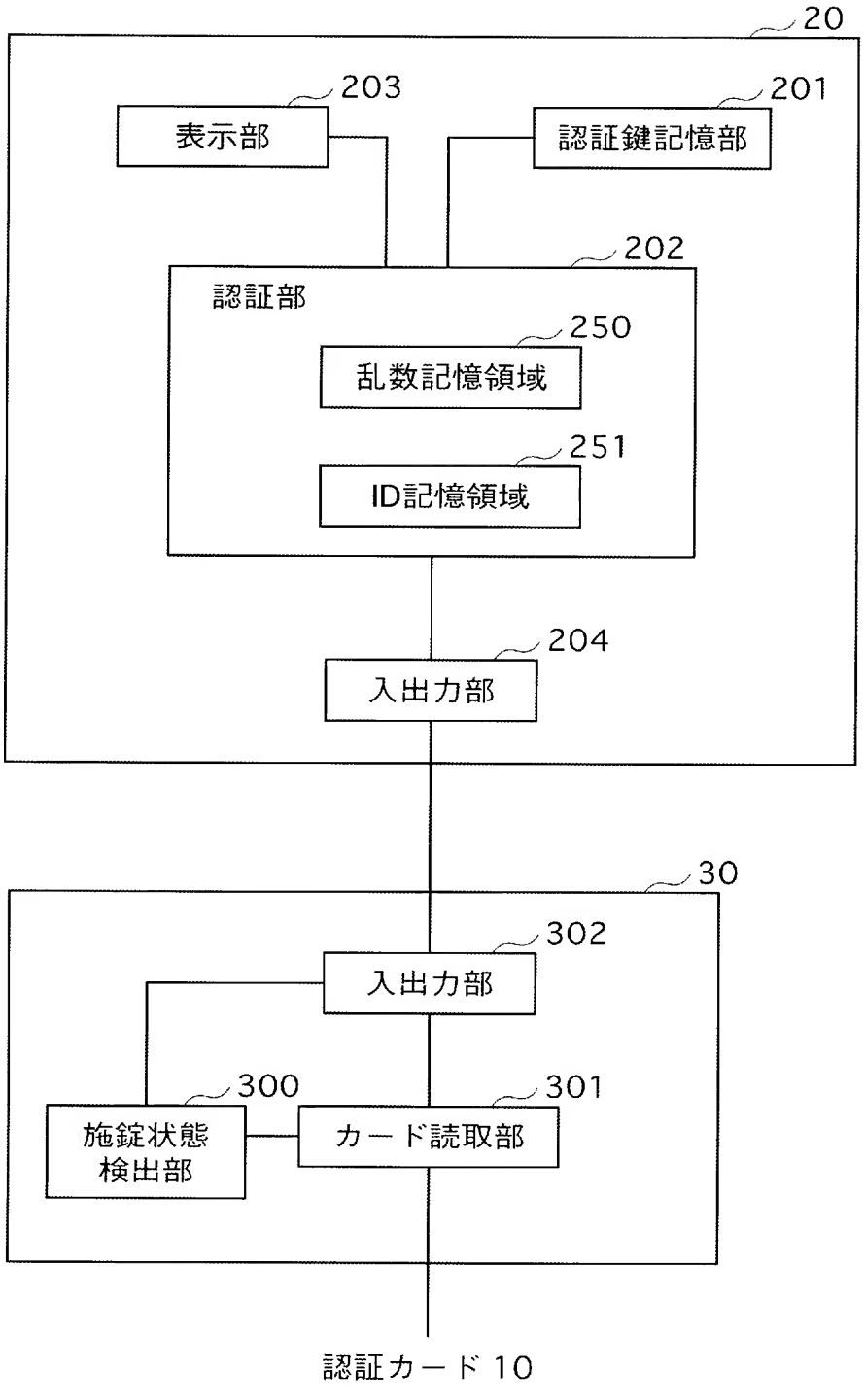
[図1]



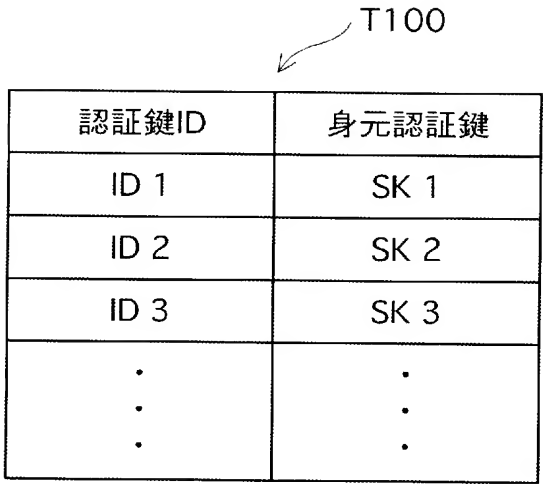
[図2]



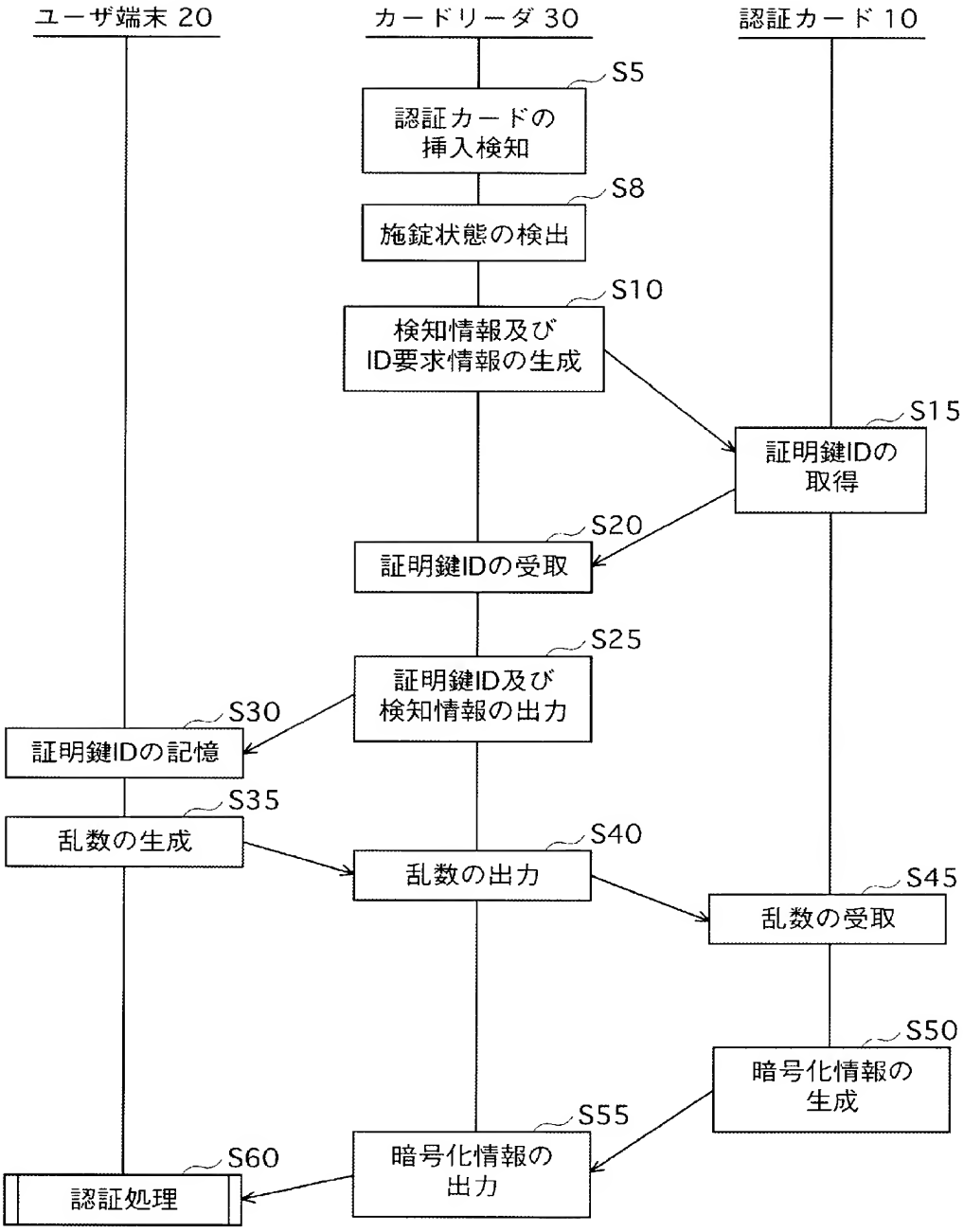
[図3]


20
203
表示部
201
認証鍵記憶部
202
認証部
250
乱数記憶領域
251
ID記憶領域
204
入出力部
30
302
入出力部
300
施錠状態
検出部
301
カード読取部
認証カード 10

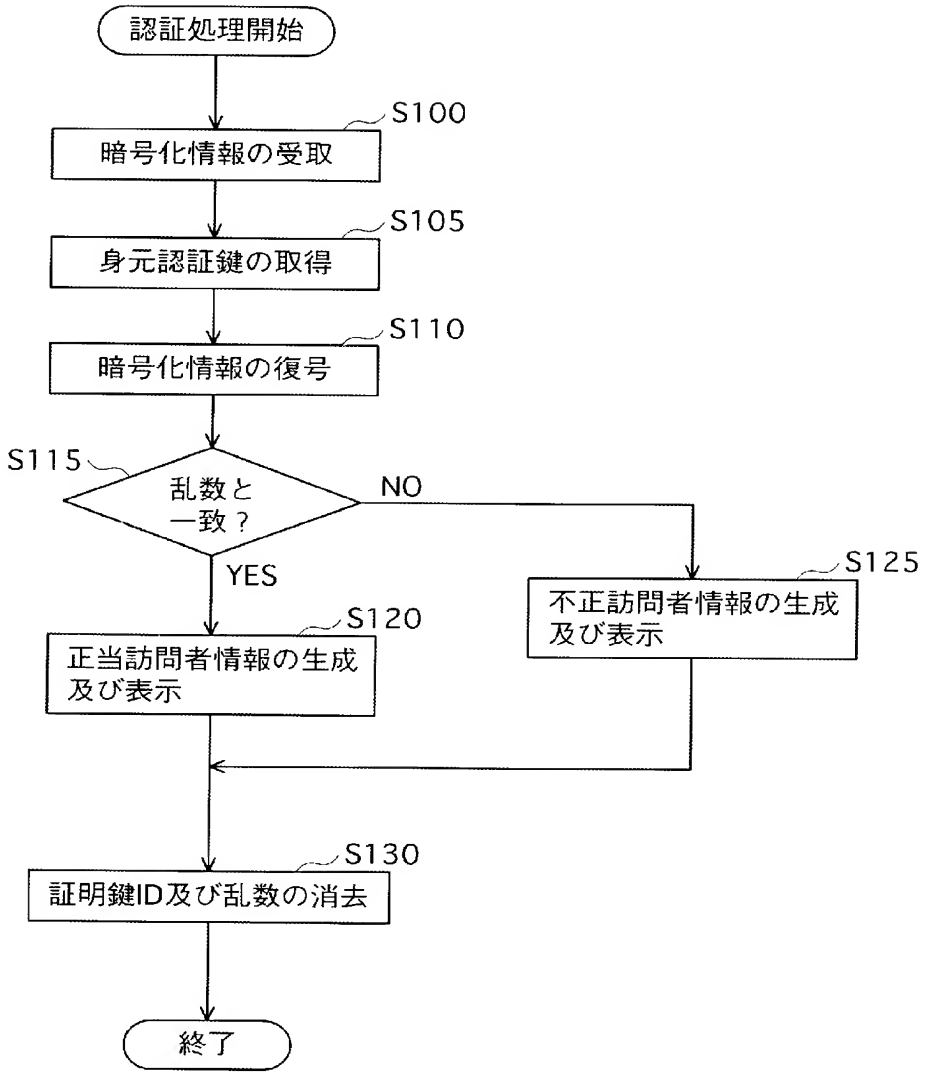
[図4]



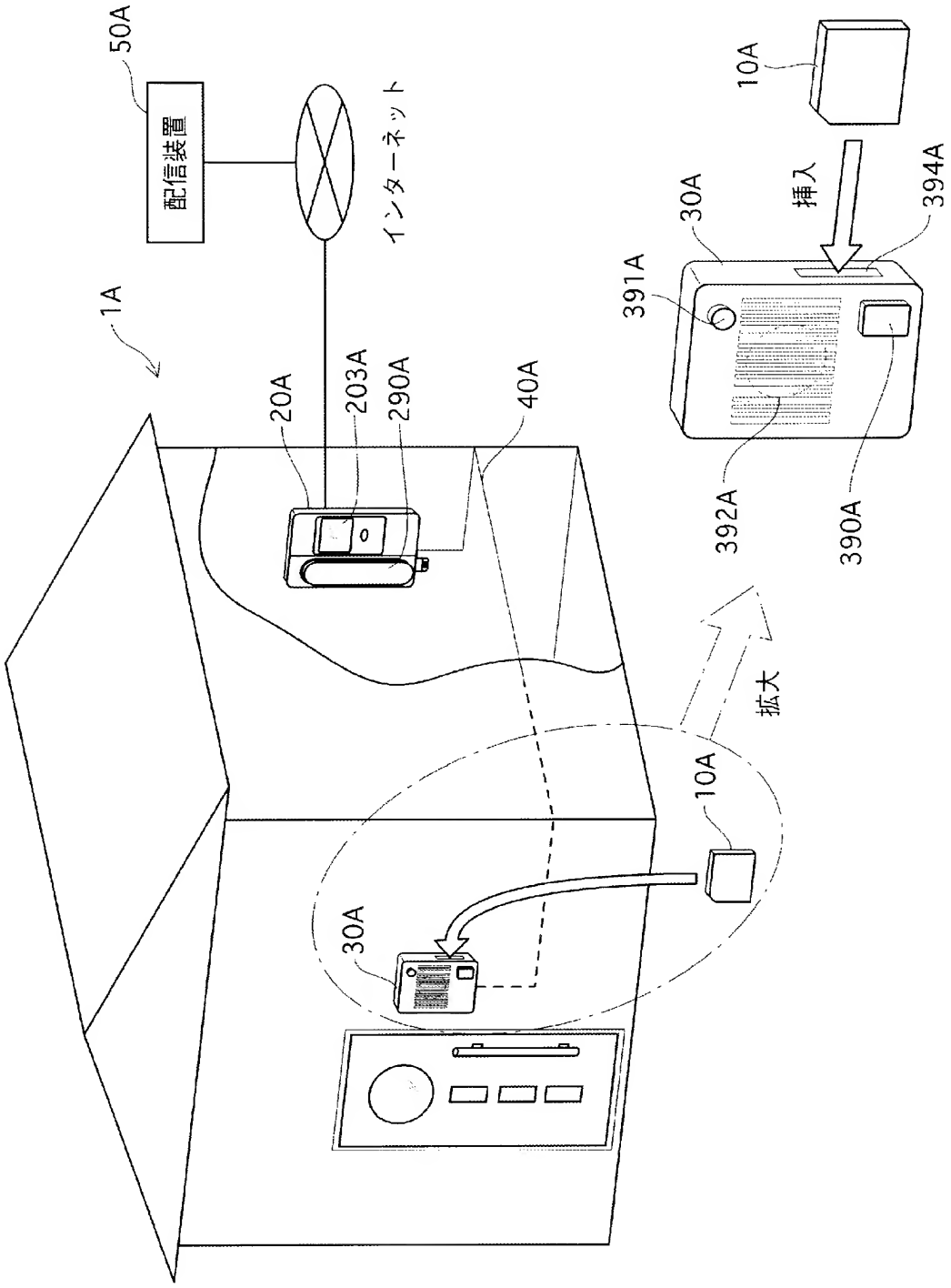
[図5]


ユーザ端末 20
カードリーダ 30
認証カード 10
S5
認証カードの挿入検知
S8
施錠状態の検出
S10
検知情報及びID要求情報の生成
S15
証明鍵IDの取得
S20
証明鍵IDの受取
S25
証明鍵ID及び検知情報の出力
S30
証明鍵IDの記憶
S35
乱数の生成
S40
乱数の出力
S45
乱数の受取
S50
暗号化情報の生成
S55
暗号化情報の出力
S60
認証処理

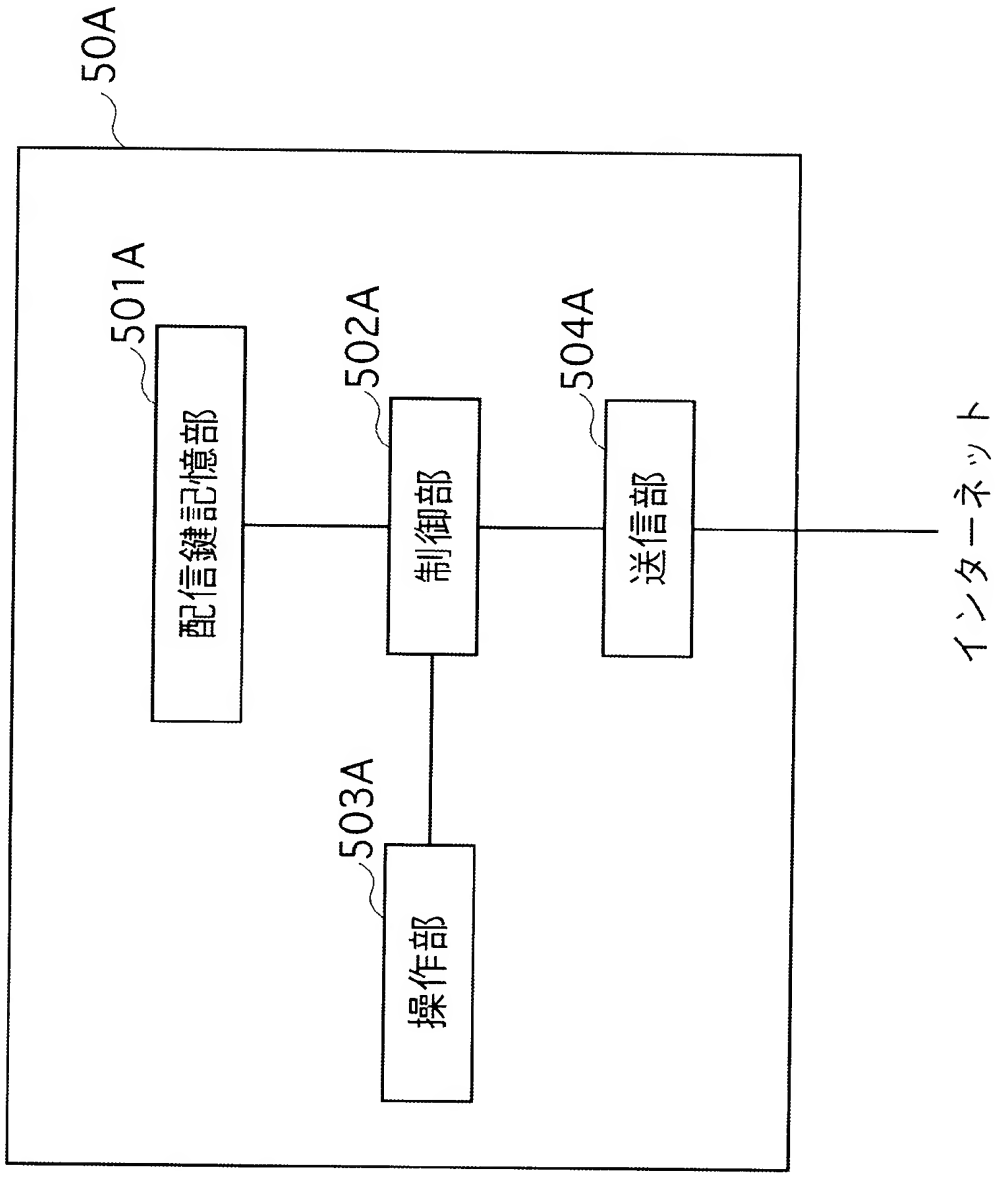
[図6]


認証処理開始
S100
暗号化情報の受取
S105
身元認証鍵の取得
S110
暗号化情報の復号
S115
乱数と一致？
NO
YES
S120
正当訪問者情報の生成及び表示
S125
不正訪問者情報の生成及び表示
S130
証明鍵ID及び乱数の消去
終了

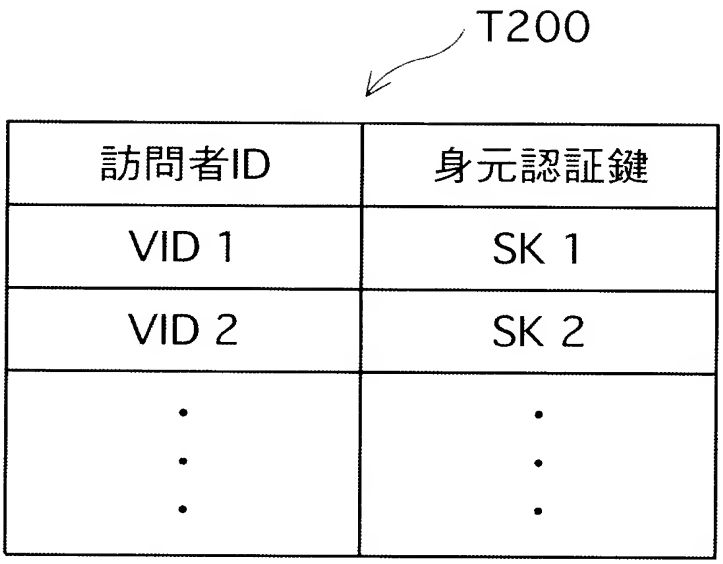
[図7]


50A
配信装置
インターネット
1A
20A
203A
290A
40A
10A
挿入
30A
394A
391A
392A
390A
拡大
10A
30A

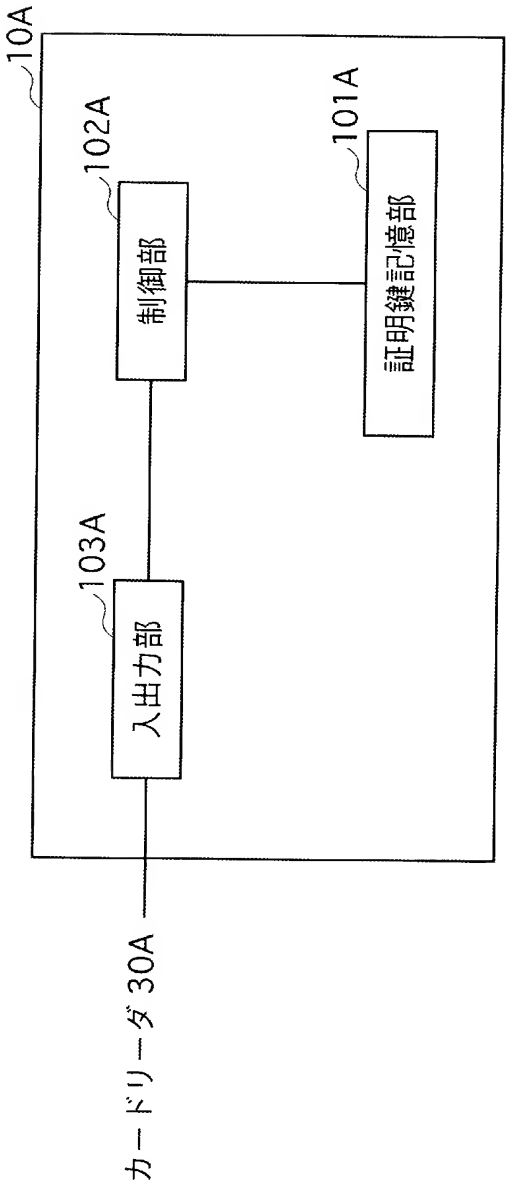
[図8]



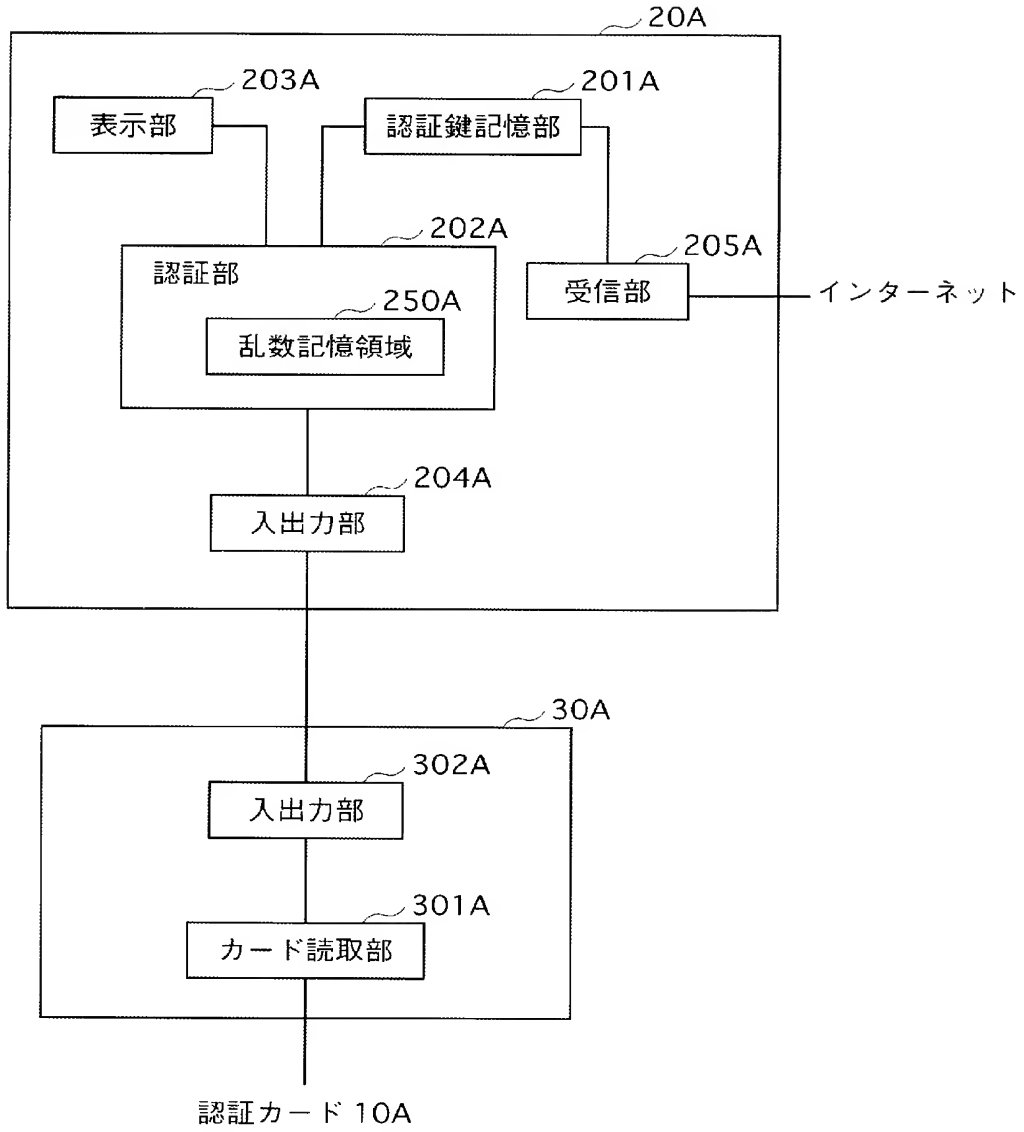
[図9]



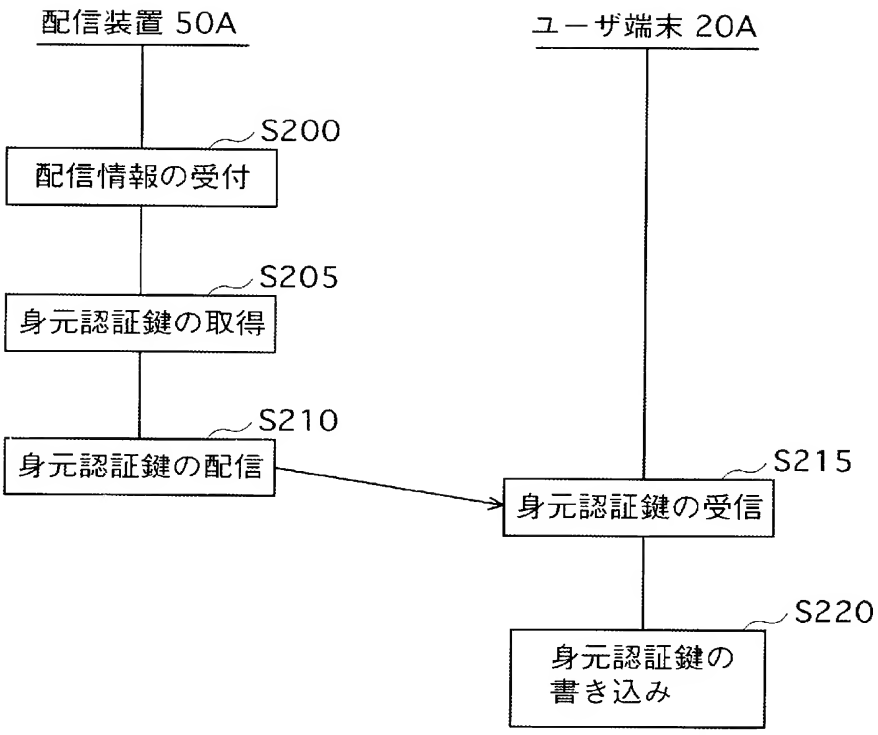
[図10]



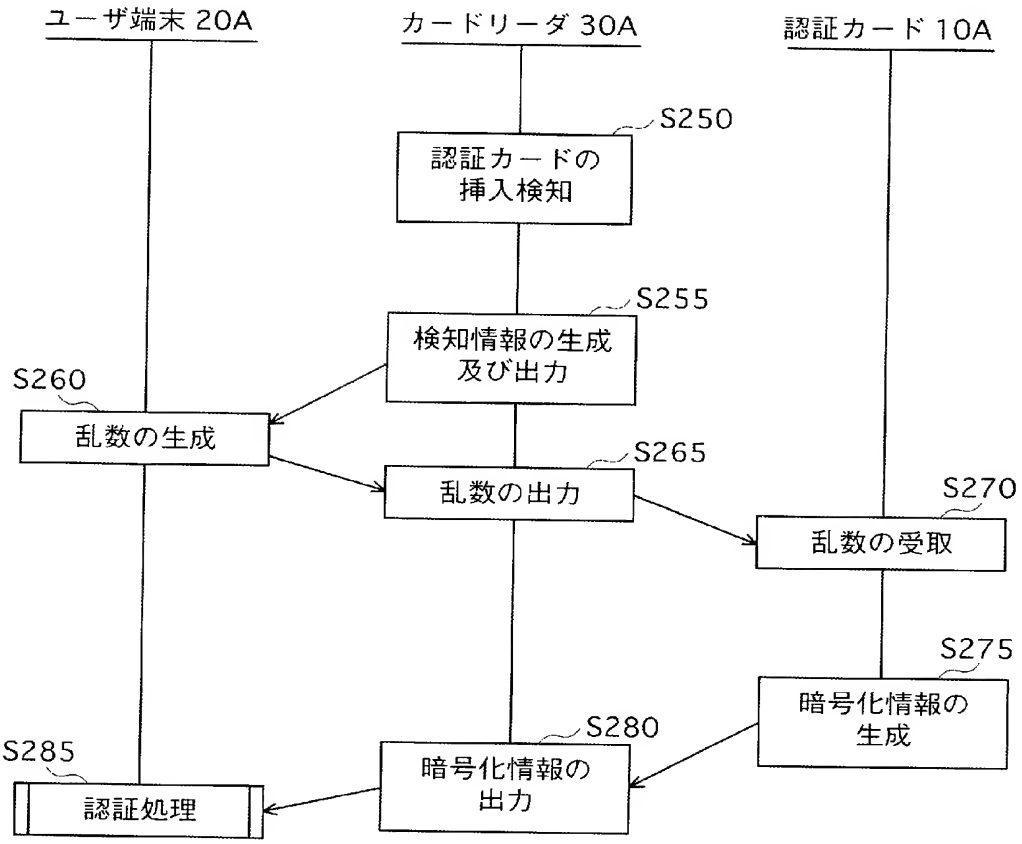
[図11]


20A
203A
表示部
201A
認証鍵記憶部
202A
認証部
250A
乱数記憶領域
205A
受信部
インターネット
204A
入出力部
30A
302A
入出力部
301A
カード読取部
認証カード 10A

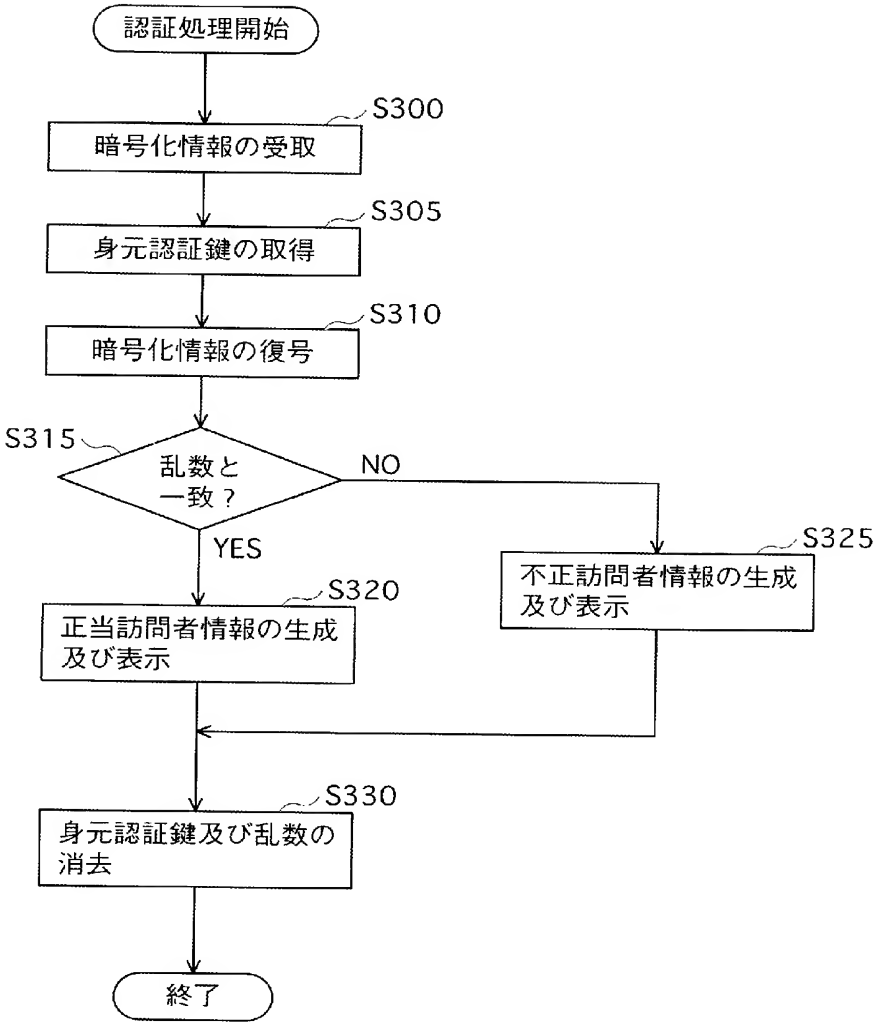
[図12]


配信装置 50A
ユーザ端末 20A
S200
配信情報の受付
S205
身元認証鍵の取得
S210
身元認証鍵の配信
S215
身元認証鍵の受信
S220
身元認証鍵の
書き込み

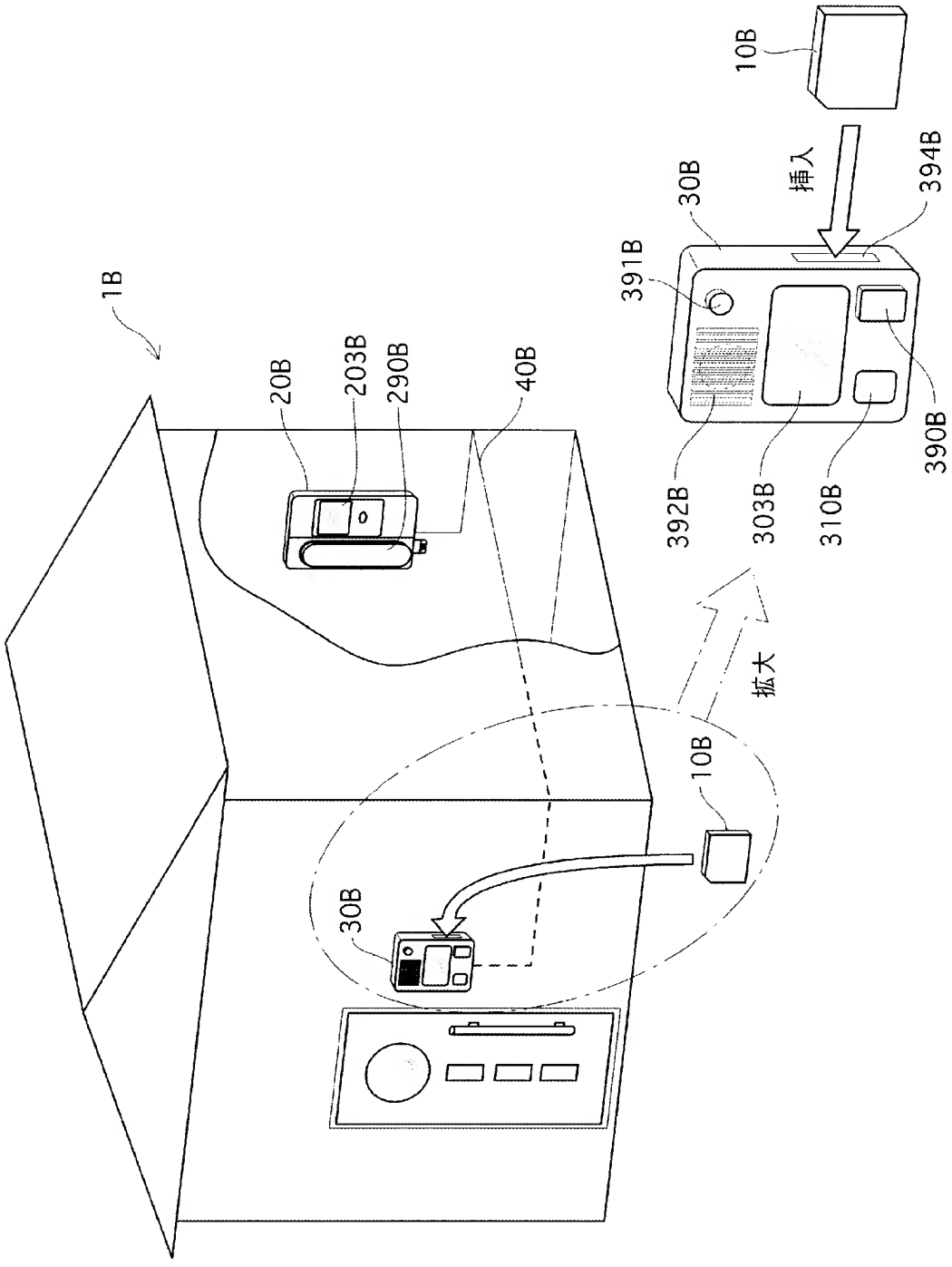
[図13]


ユーザ端末 20A
カードリーダ 30A
認証カード 10A
S250
認証カードの挿入検知
S255
検知情報の生成及び出力
S260
乱数の生成
S265
乱数の出力
S270
乱数の受取
S275
暗号化情報の生成
S280
暗号化情報の出力
S285
認証処理

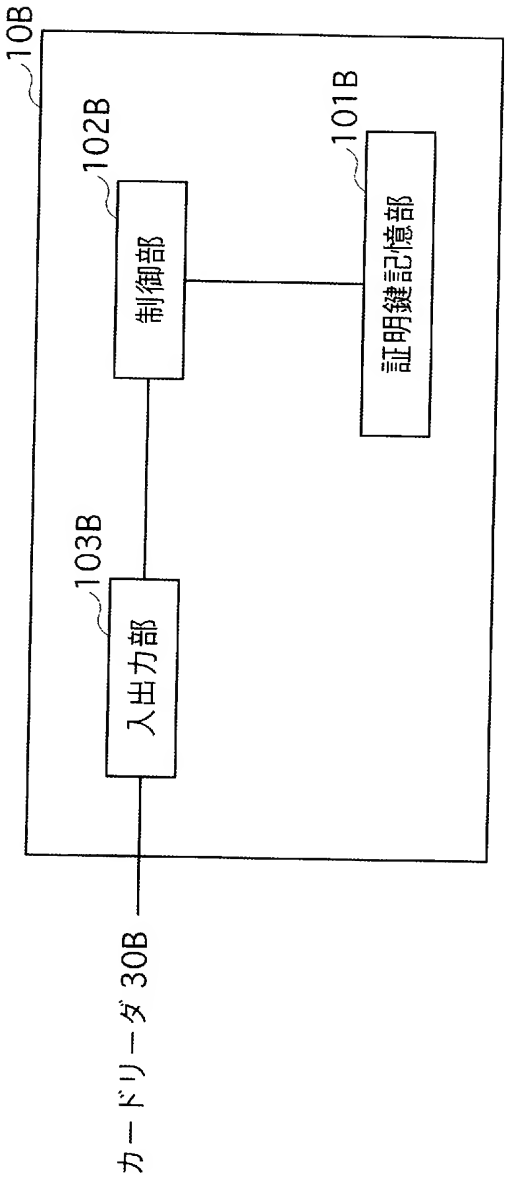
[図14]


認証処理開始
S300
暗号化情報の受取
S305
身元認証鍵の取得
S310
暗号化情報の復号
S315
乱数と一致？
NO
YES
S320
正当訪問者情報の生成及び表示
S325
不正訪問者情報の生成及び表示
S330
身元認証鍵及び乱数の消去
終了

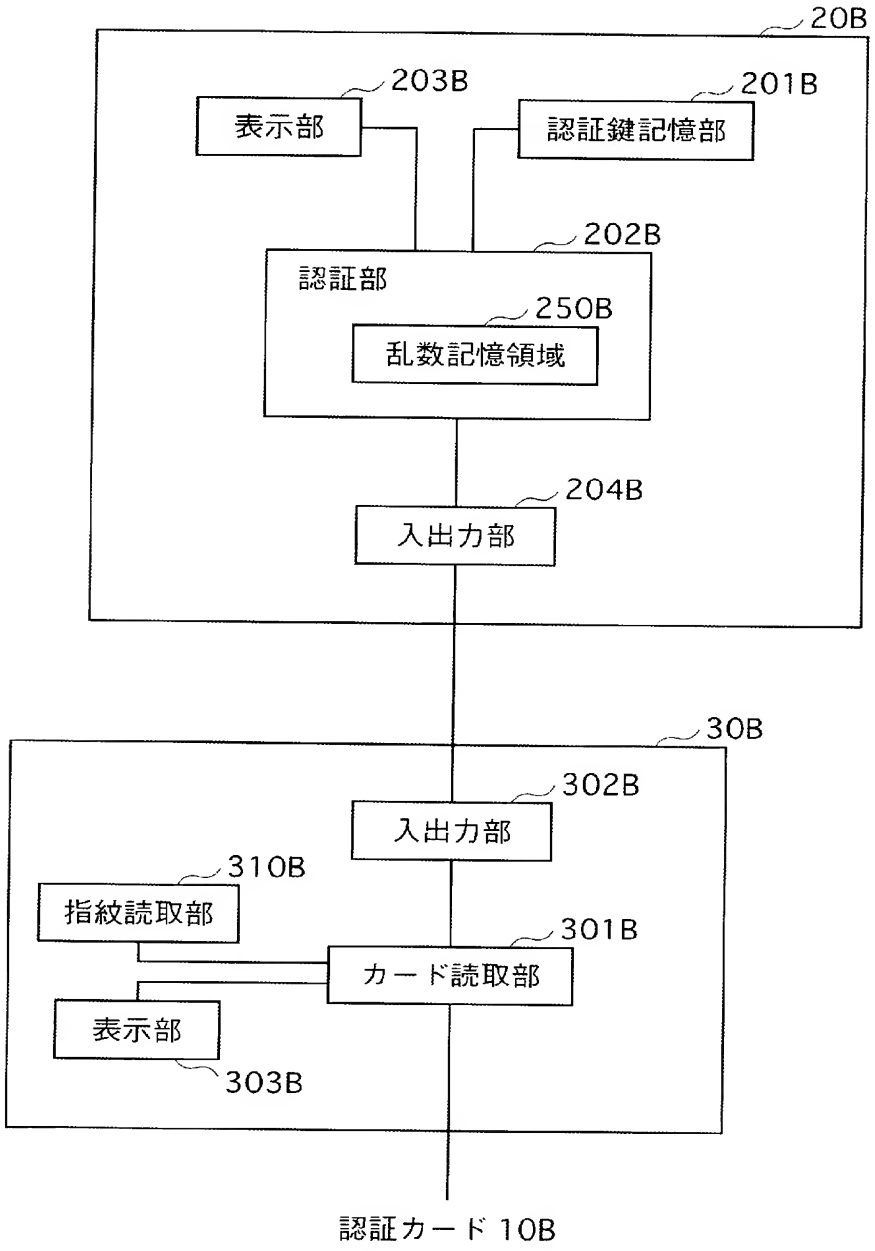
[図15]


10B
挿入
394B
30B
391B
1B
20B
203B
290B
40B
390B
392B
303B
310B
拡大
10B
30B

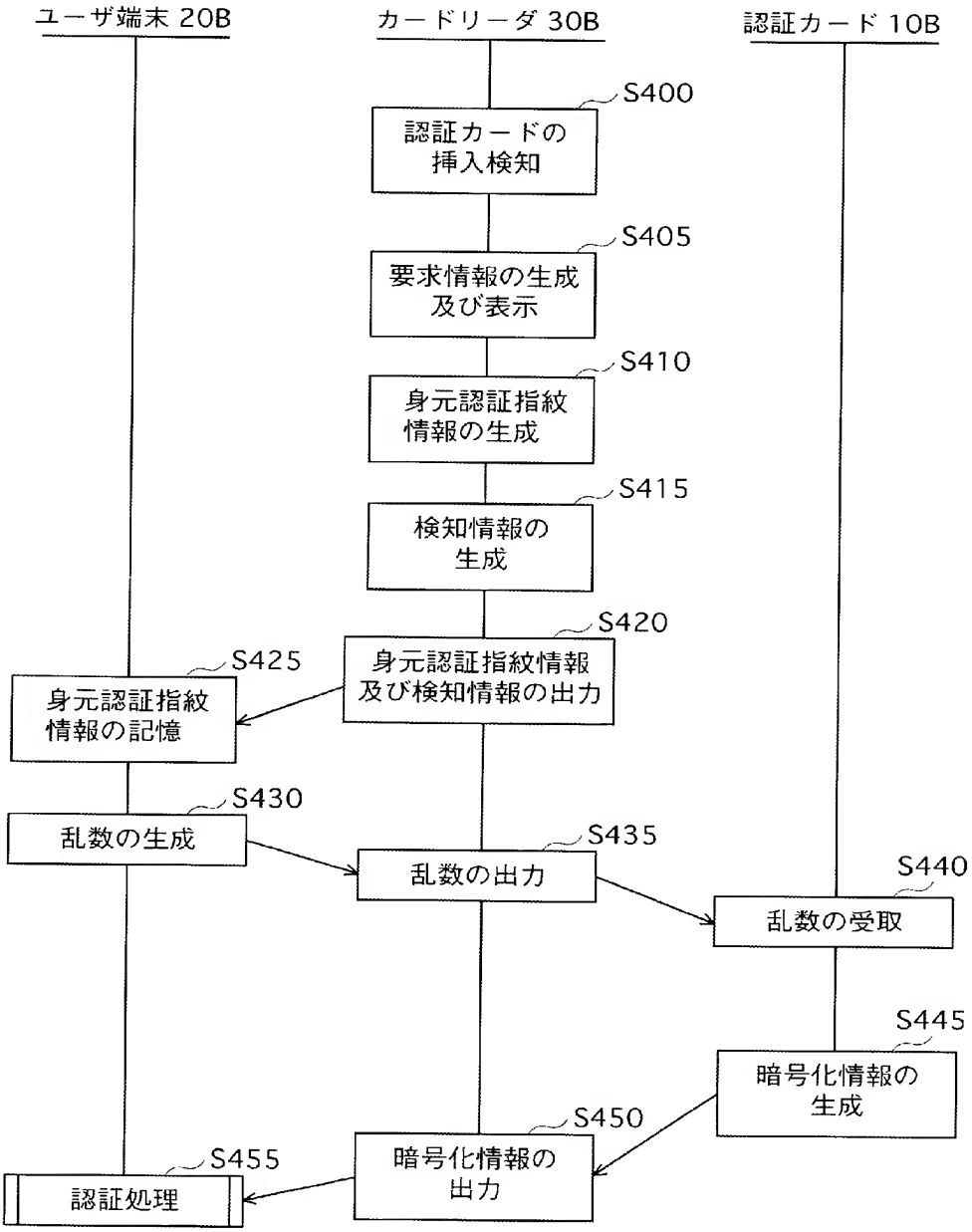
[図16]



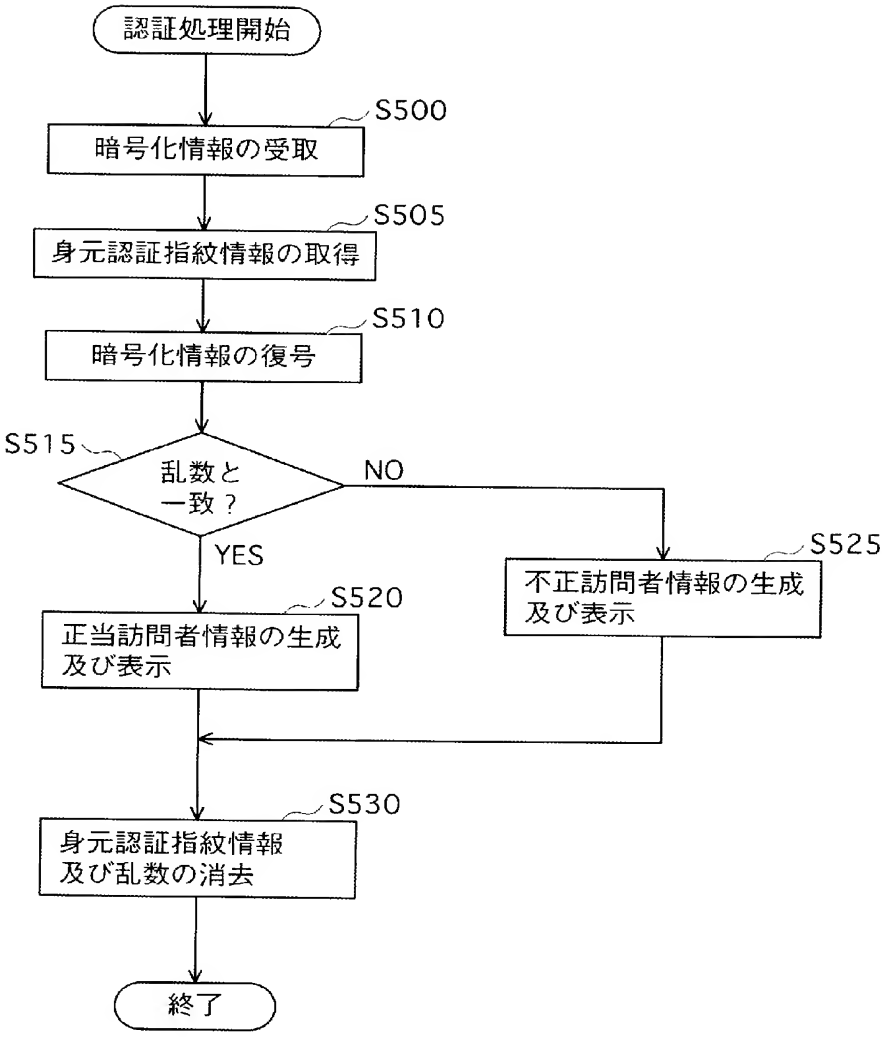
[図17]


20B
203B
表示部
201B
認証鍵記憶部
202B
認証部
250B
乱数記憶領域
204B
入出力部
30B
302B
入出力部
310B
指紋読取部
301B
カード読取部
表示部
303B
認証カード 10B

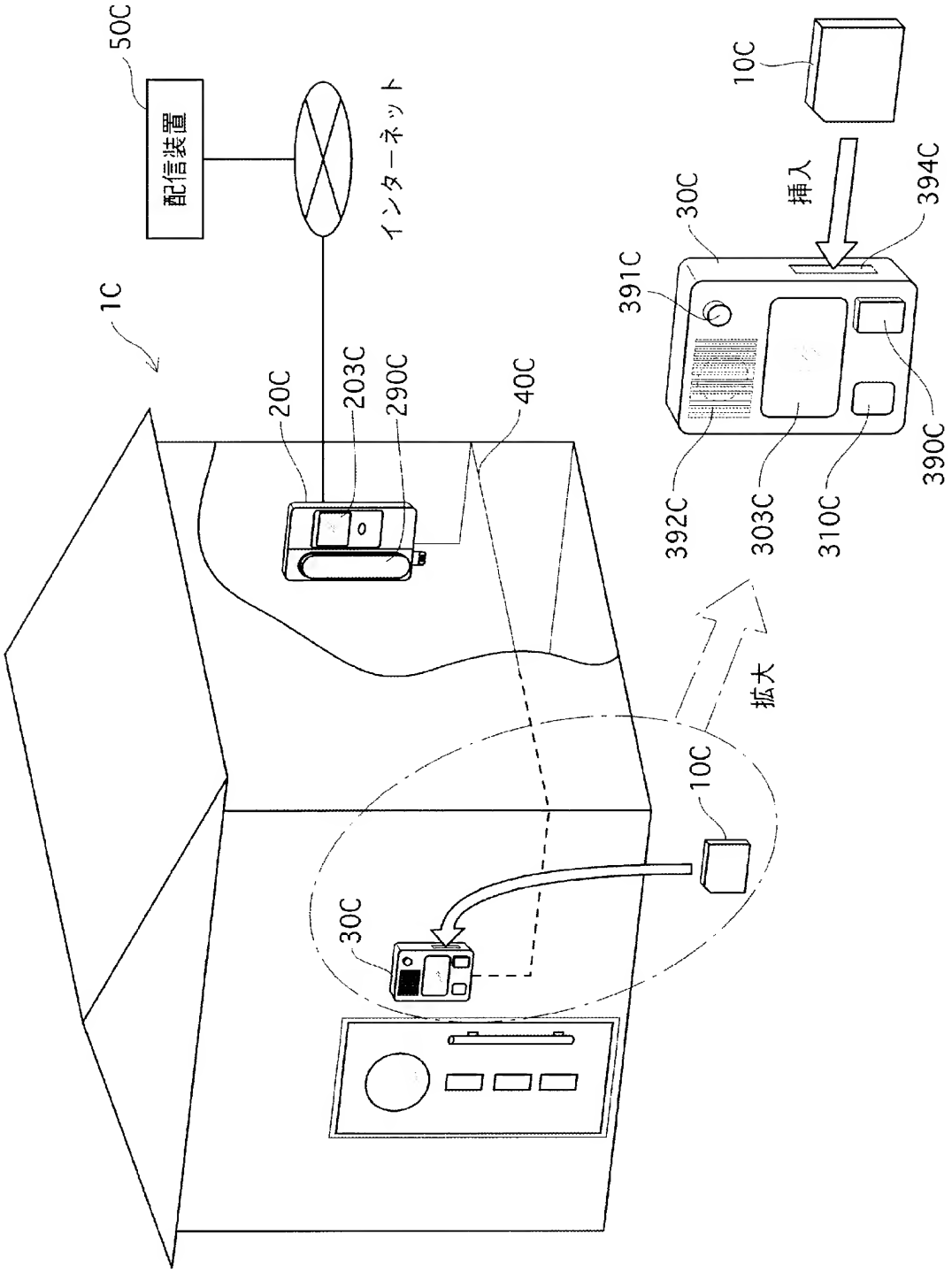
[図18]


ユーザ端末 20B
カードリーダ 30B
認証カード 10B
S400
認証カードの挿入検知
S405
要求情報の生成及び表示
S410
身元認証指紋情報の生成
S415
検知情報の生成
S420
身元認証指紋情報及び検知情報の出力
S425
身元認証指紋情報の記憶
S430
乱数の生成
S435
乱数の出力
S440
乱数の受取
S445
暗号化情報の生成
S450
暗号化情報の出力
S455
認証処理

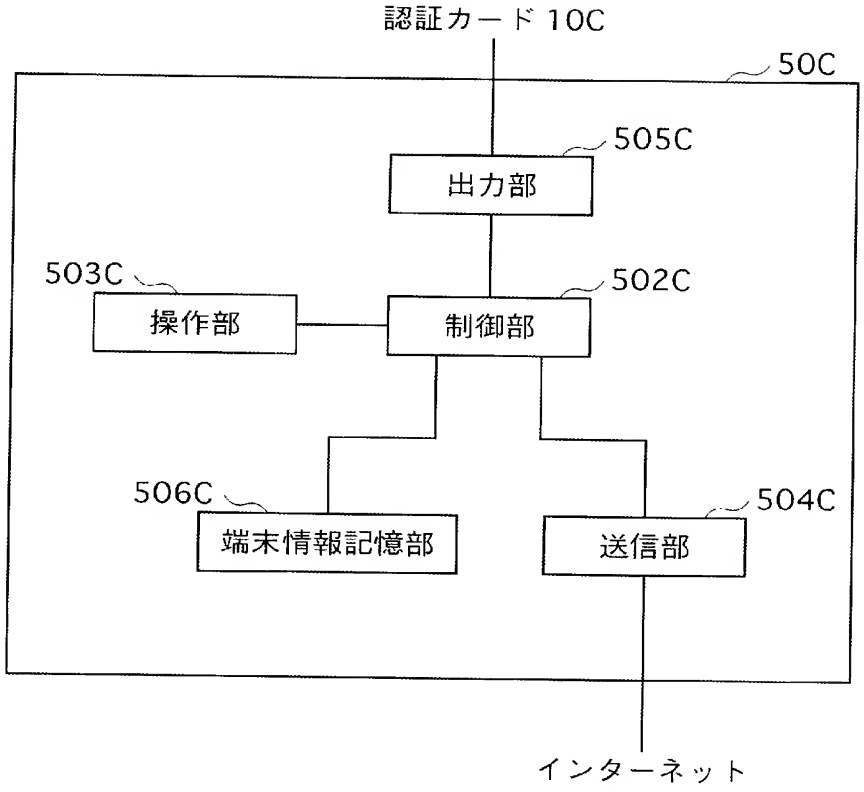
[図19]


認証処理開始
S500
暗号化情報の受取
S505
身元認証指紋情報の取得
S510
暗号化情報の復号
S515
乱数と
一致？
NO
YES
S520
正当訪問者情報の生成
及び表示
S525
不正訪問者情報の生成
及び表示
S530
身元認証指紋情報
及び乱数の消去
終了

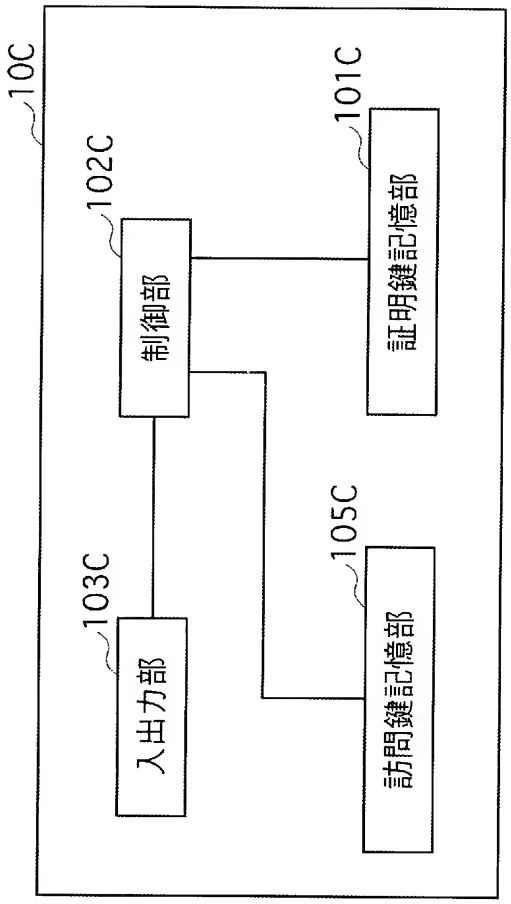
[図20]


50C
配信装置
インターネット
1C
20C
203C
290C
40C
10C
挿入
394C
30C
391C
390C
392C
303C
310C
拡大
10C
30C

[図21]


認証カード10C
50C
505C
出力部
503C
操作部
502C
制御部
506C
端末情報記憶部
504C
送信部
インターネット

[図22]



[図23]

(a)

T300

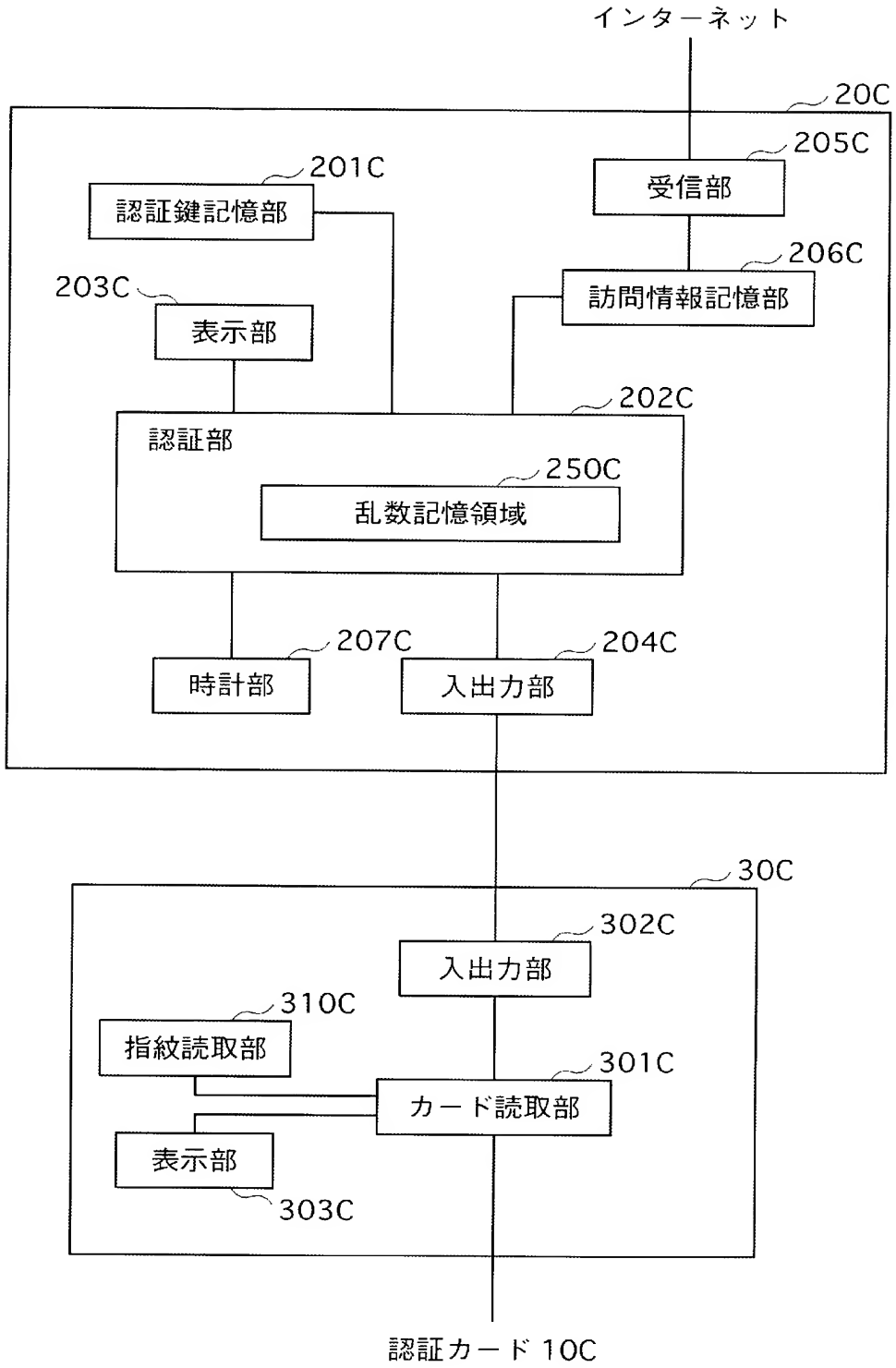
端末ID	訪問時間帯	訪問内容
T-ID 1	13:00～15:00	物品A届
T-ID 2	13:00～15:00	物品B届
・ ・ ・	・ ・ ・	・ ・ ・

(b)

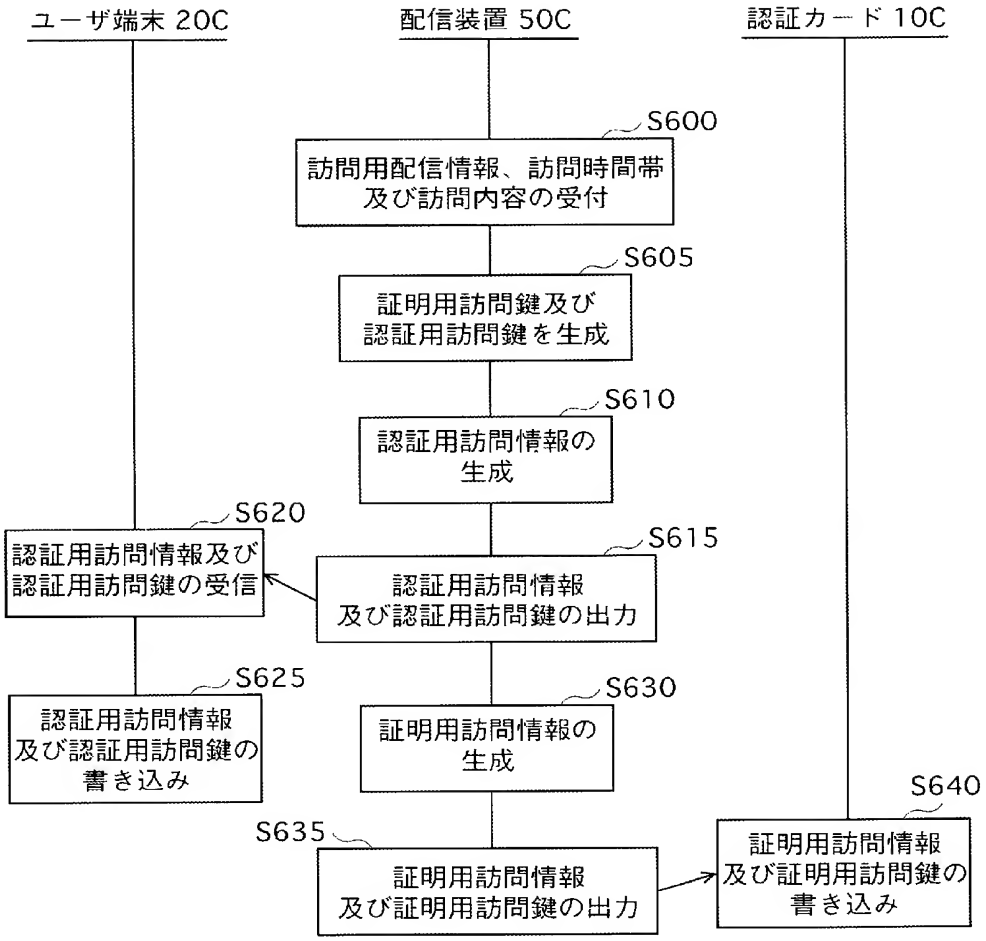
T310

端末ID	訪問鍵
T-ID 1	V-key1
T-ID 2	V-key2
・ ・ ・	・ ・ ・

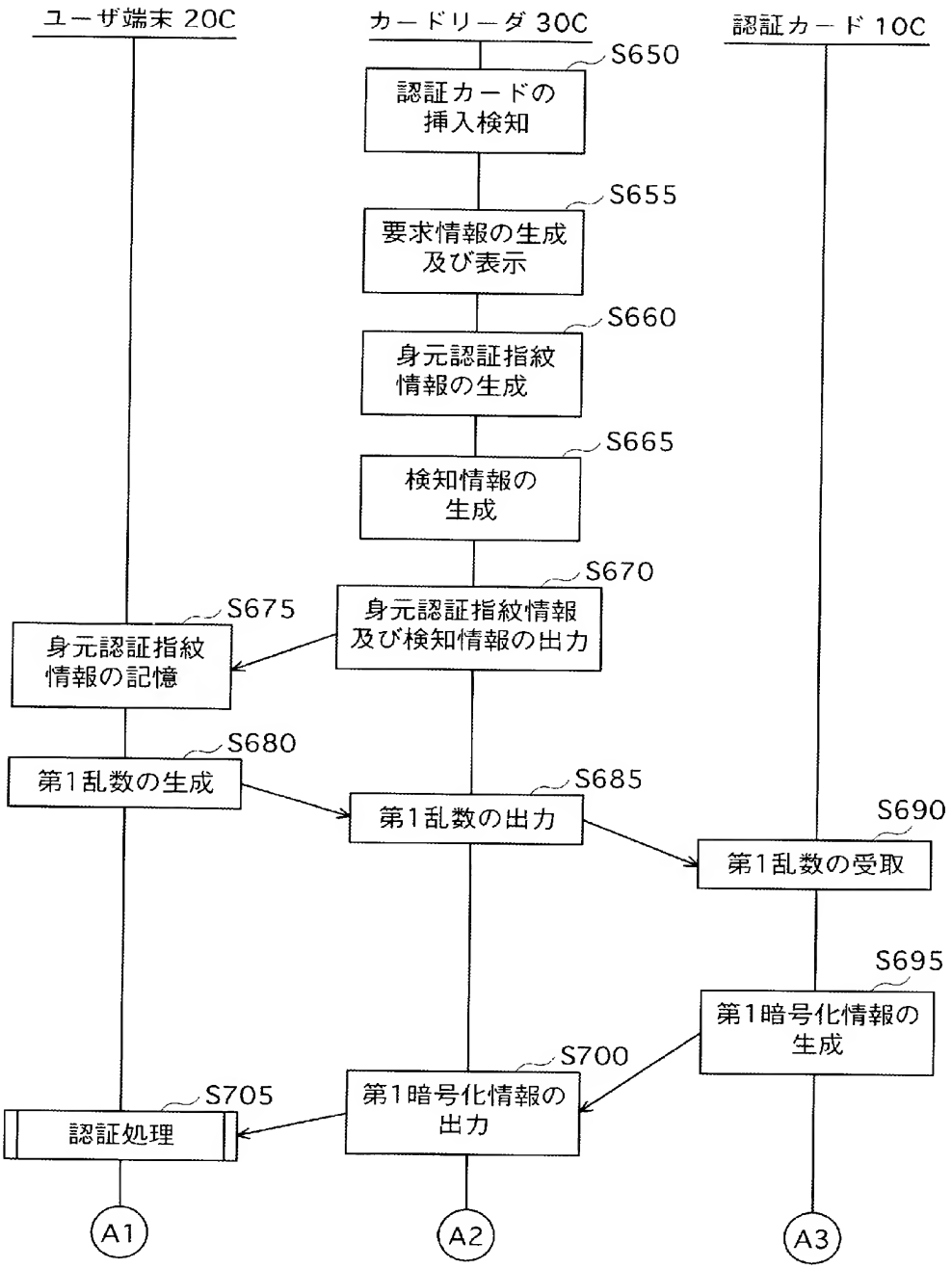
[図24]


インターネット
20C
205C
受信部
201C
認証鍵記憶部
206C
訪問情報記憶部
203C
表示部
202C
認証部
250C
乱数記憶領域
207C
時計部
204C
入出力部
30C
302C
入出力部
310C
指紋読取部
301C
カード読取部
表示部
303C
認証カード 10C

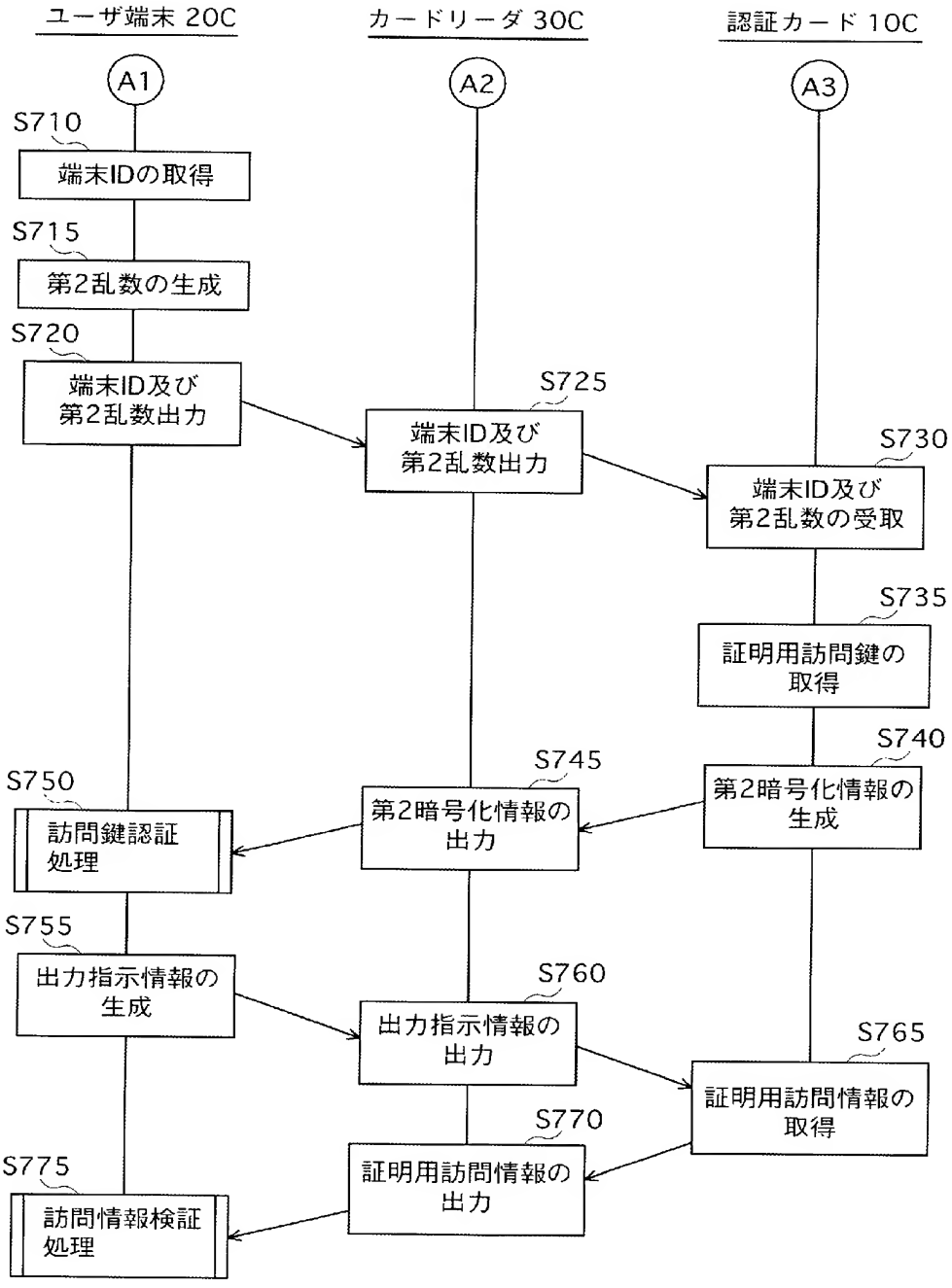
[図25]


ユーザ端末 20C
配信装置 50C
認証カード 10C
S600
訪問用配信情報、訪問時間帯及び訪問内容の受付
S605
証明用訪問鍵及び認証用訪問鍵を生成
S610
認証用訪問情報の生成
S620
認証用訪問情報及び認証用訪問鍵の受信
S615
認証用訪問情報及び認証用訪問鍵の出力
S625
認証用訪問情報及び認証用訪問鍵の書き込み
S630
証明用訪問情報の生成
S640
S635
証明用訪問情報及び証明用訪問鍵の出力
証明用訪問情報及び証明用訪問鍵の書き込み

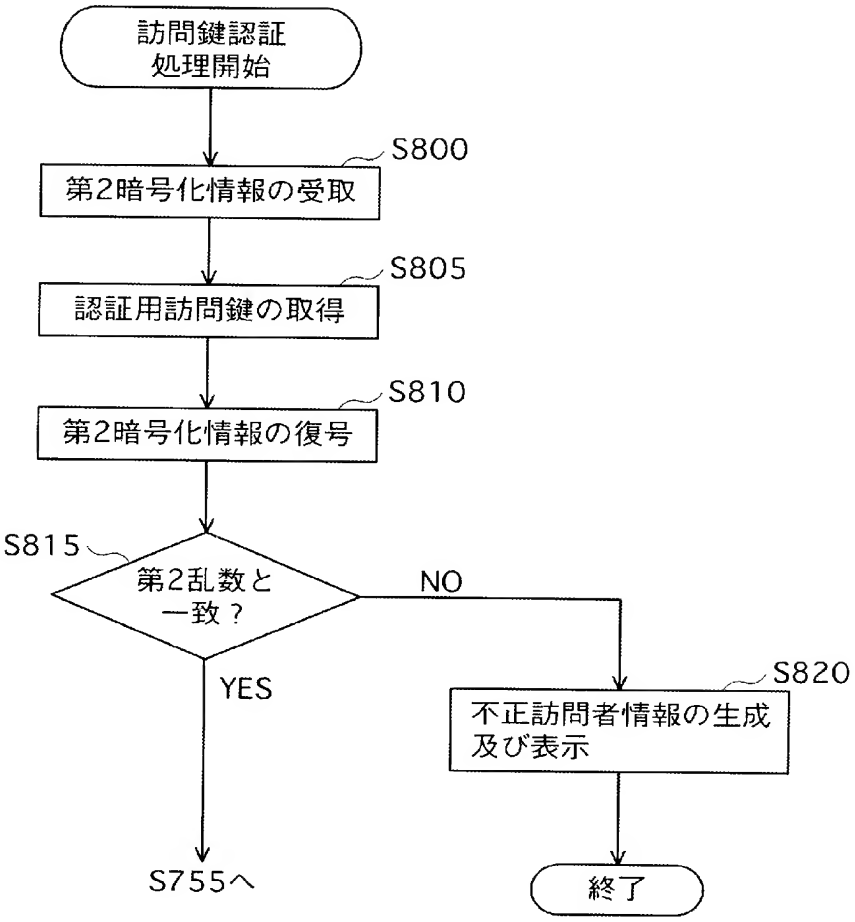
[図26]


ユーザ端末 20C
カードリーダ 30C
認証カード 10C
S650
認証カードの挿入検知
S655
要求情報の生成及び表示
S660
身元認証指紋情報の生成
S665
検知情報の生成
S670
身元認証指紋情報及び検知情報の出力
S675
身元認証指紋情報の記憶
S680
第1乱数の生成
S685
第1乱数の出力
S690
第1乱数の受取
S695
第1暗号化情報の生成
S700
第1暗号化情報の出力
S705
認証処理
A1
A2
A3

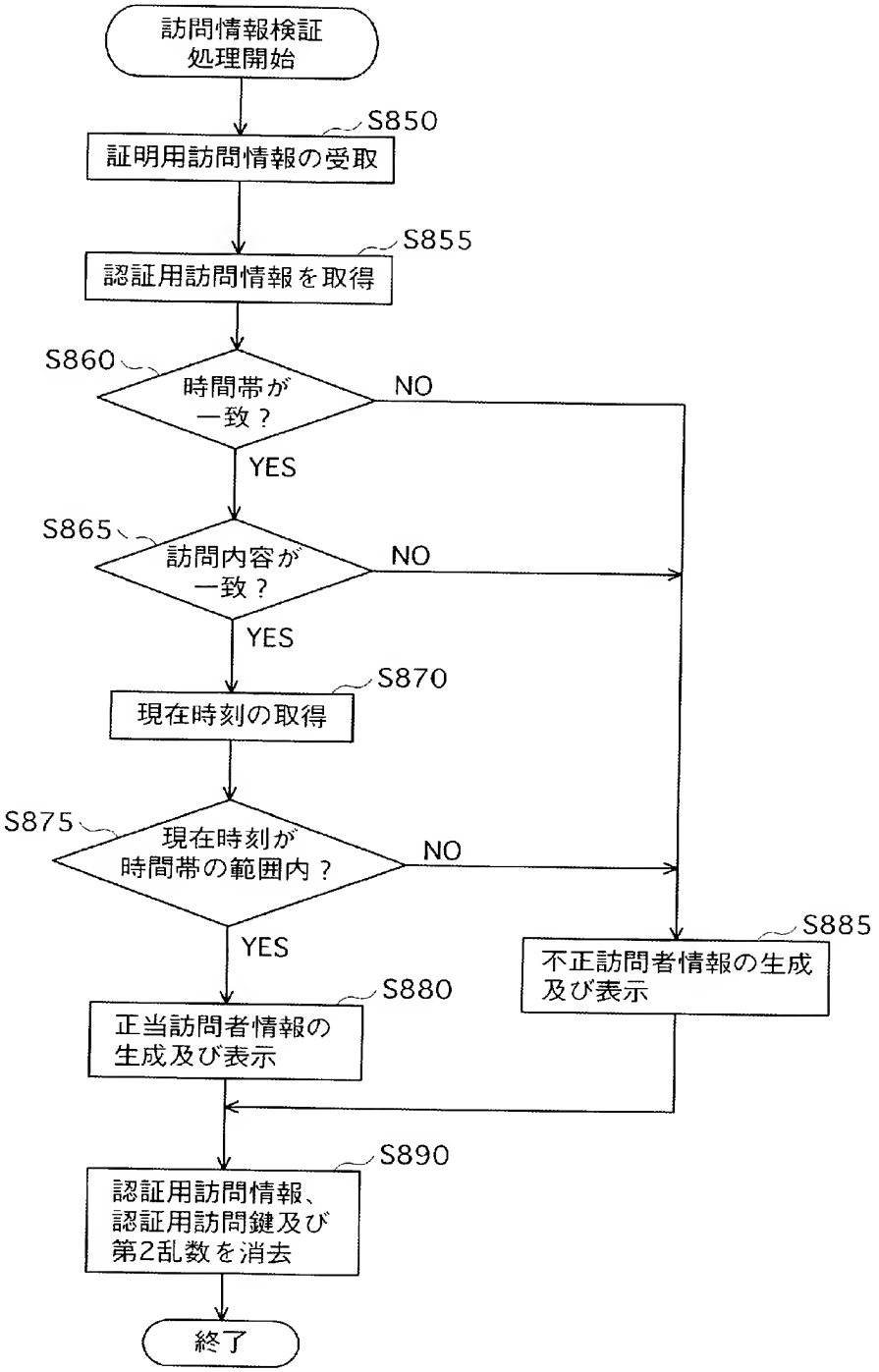
[図27]


ユーザ端末 20C
カードリーダ 30C
認証カード 10C
A1
A2
A3
S710
端末IDの取得
S715
第2乱数の生成
S720
端末ID及び
第2乱数出力
S725
端末ID及び
第2乱数出力
S730
端末ID及び
第2乱数の受取
S735
証明用訪問鍵の
取得
S740
第2暗号化情報の
生成
S745
第2暗号化情報の
出力
S750
訪問鍵認証
処理
S755
出力指示情報の
生成
S760
出力指示情報の
出力
S765
証明用訪問情報の
取得
S770
証明用訪問情報の
出力
S775
訪問情報検証
処理

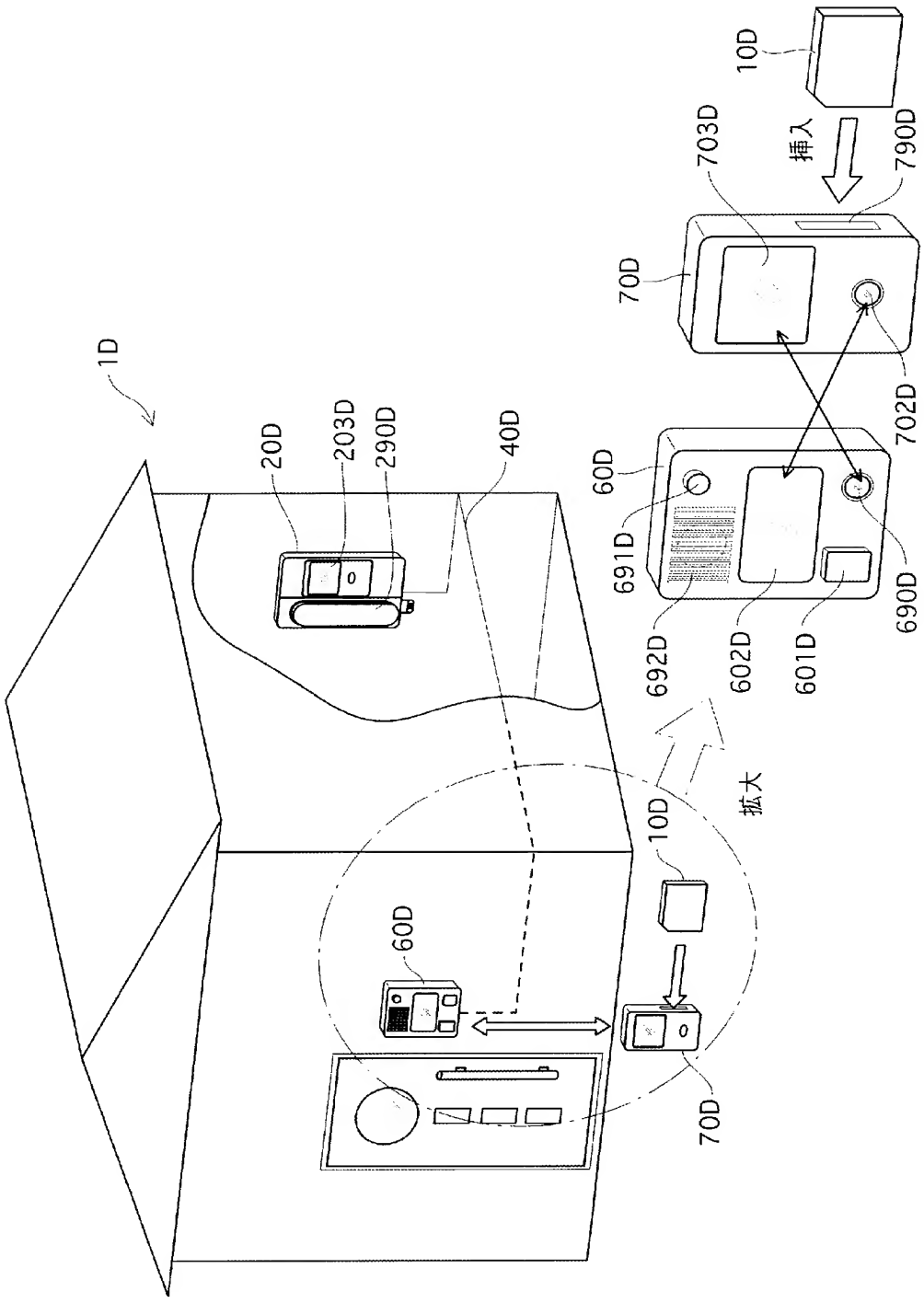
[図28]


訪問鍵認証
処理開始
S800
第2暗号化情報の受取
S805
認証用訪問鍵の取得
S810
第2暗号化情報の復号
S815
第2乱数と
一致？
NO
YES
S820
不正訪問者情報の生成
及び表示
S755へ
終了

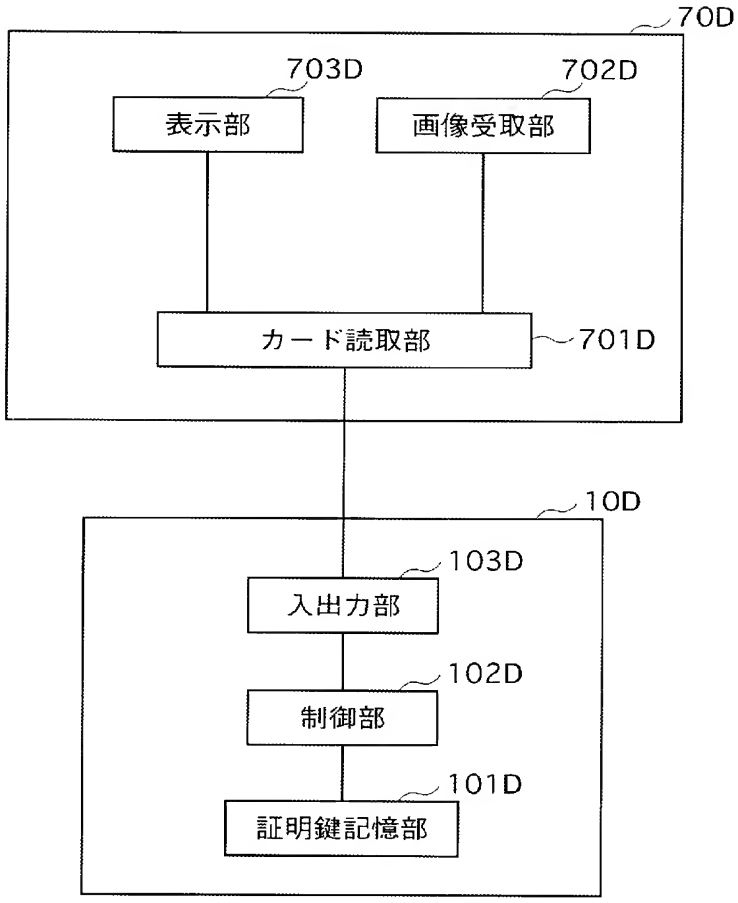
[図29]


訪問情報検証処理開始
S850
証明用訪問情報の受取
S855
認証用訪問情報を取得
S860
時間帯が一致？
NO
YES
S865
訪問内容が一致？
NO
YES
S870
現在時刻の取得
S875
現在時刻が時間帯の範囲内？
NO
YES
S885
不正訪問者情報の生成及び表示
S880
正当訪問者情報の生成及び表示
S890
認証用訪問情報、認証用訪問鍵及び第2乱数を消去
終了

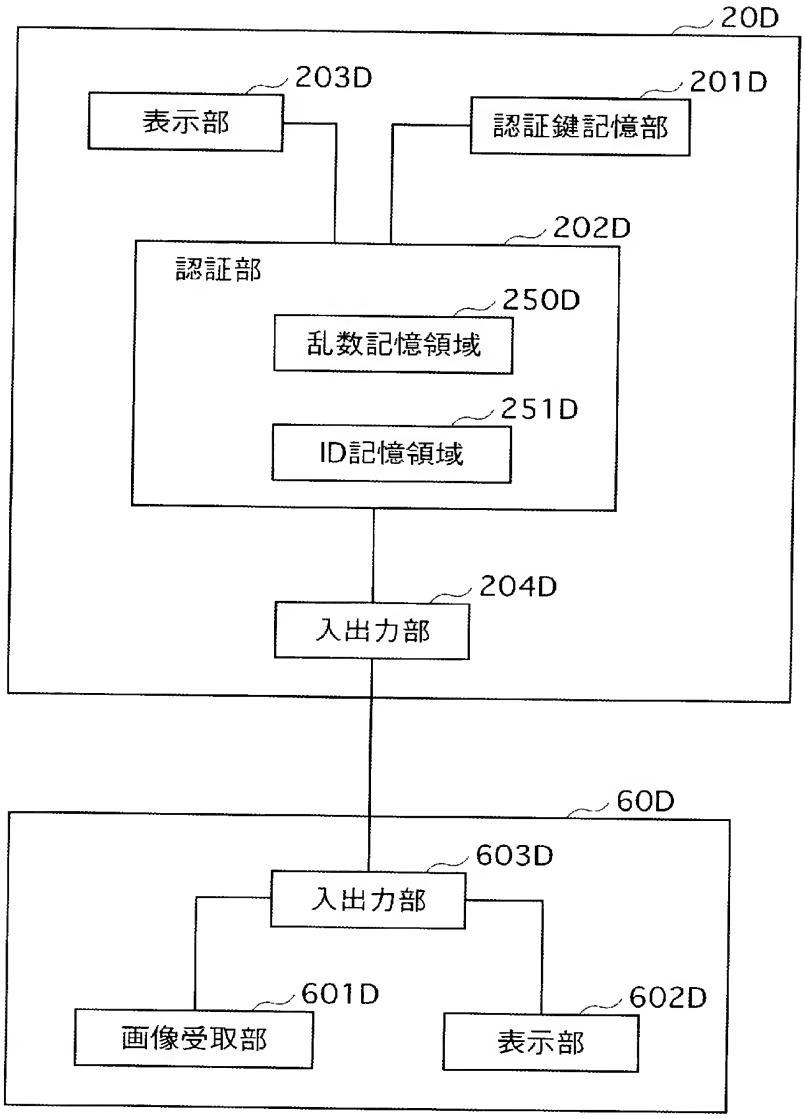
[図30]


1D
20D
203D
290D
40D
10D
挿入
703D
790D
70D
702D
60D
691D
692D
602D
601D
690D
拡大
10D
60D
70D

[図31]


70D
703D
表示部
702D
画像受取部
カード読取部
701D
10D
103D
入出力部
102D
制御部
101D
証明鍵記憶部

[図32]


20D
203D
表示部
201D
認証鍵記憶部
202D
認証部
250D
乱数記憶領域
251D
ID記憶領域
204D
入出力部
60D
603D
入出力部
601D
画像受取部
602D
表示部

[図33]

T500

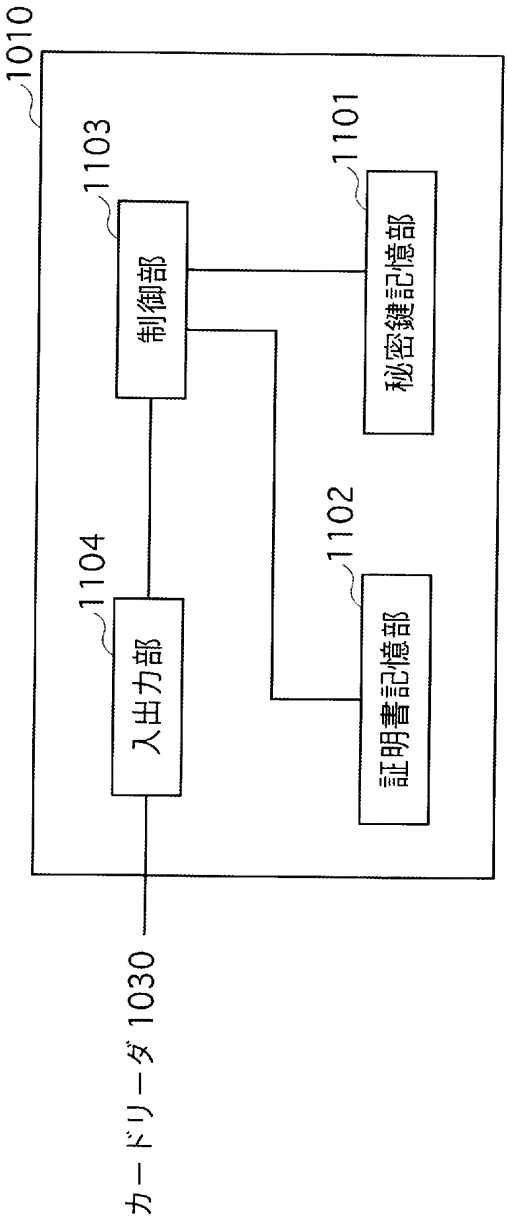
認証鍵ID	身元認証鍵	一方向性関数
ID 1	SK 1	f_1
ID 2	SK 2	f_2
ID 3	SK 3	f_3
・ ・ ・	・ ・ ・	・ ・ ・

[図34]

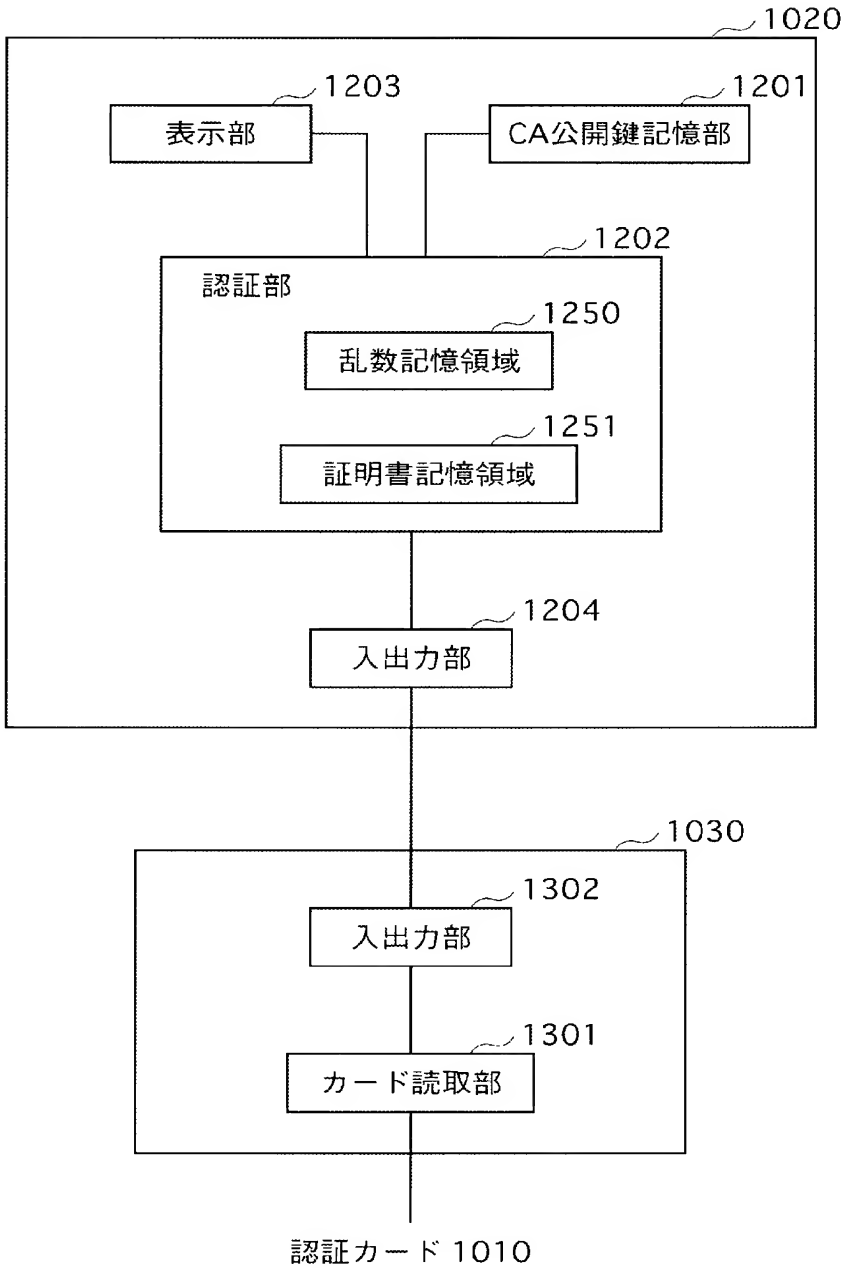
T600

認証用関数ID	一方向性関数
ID_1	f_1
ID_2	f_2
ID_3	f_3
・ ・ ・	・ ・ ・

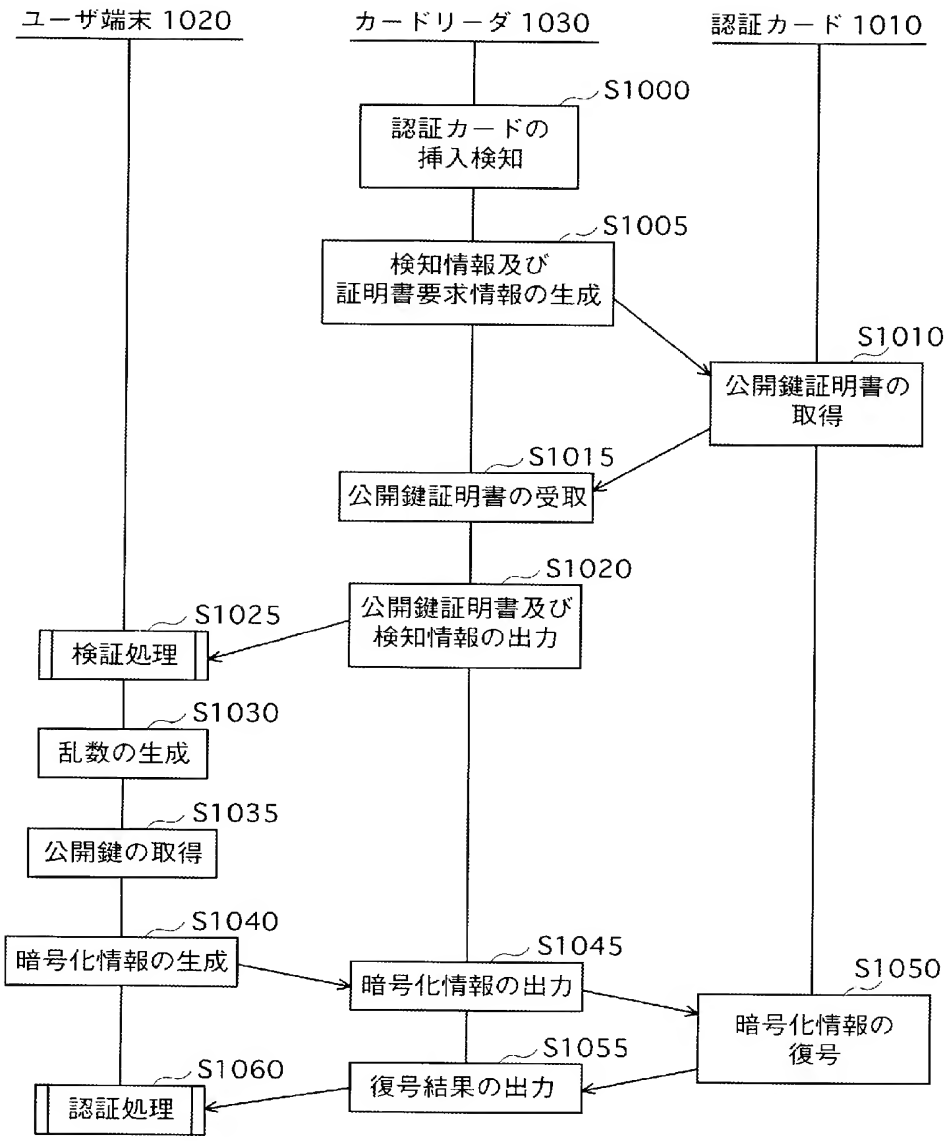
[図35]



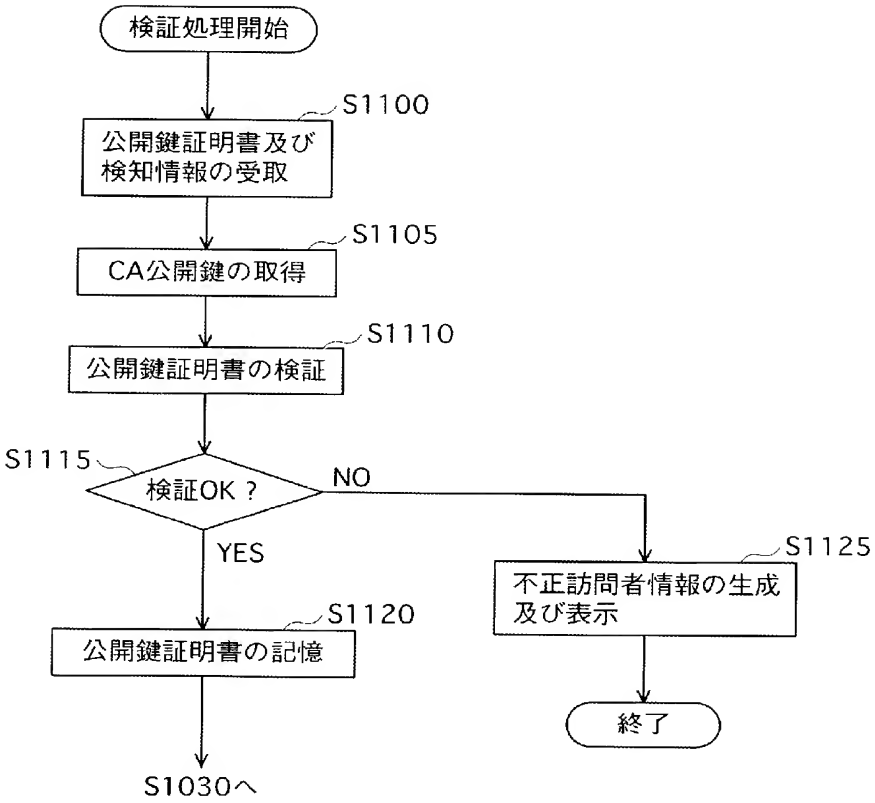
[図36]


1020
1203
表示部
1201
CA公開鍵記憶部
1202
認証部
1250
乱数記憶領域
1251
証明書記憶領域
1204
入出力部
1030
1302
入出力部
1301
カード読取部
認証カード 1010

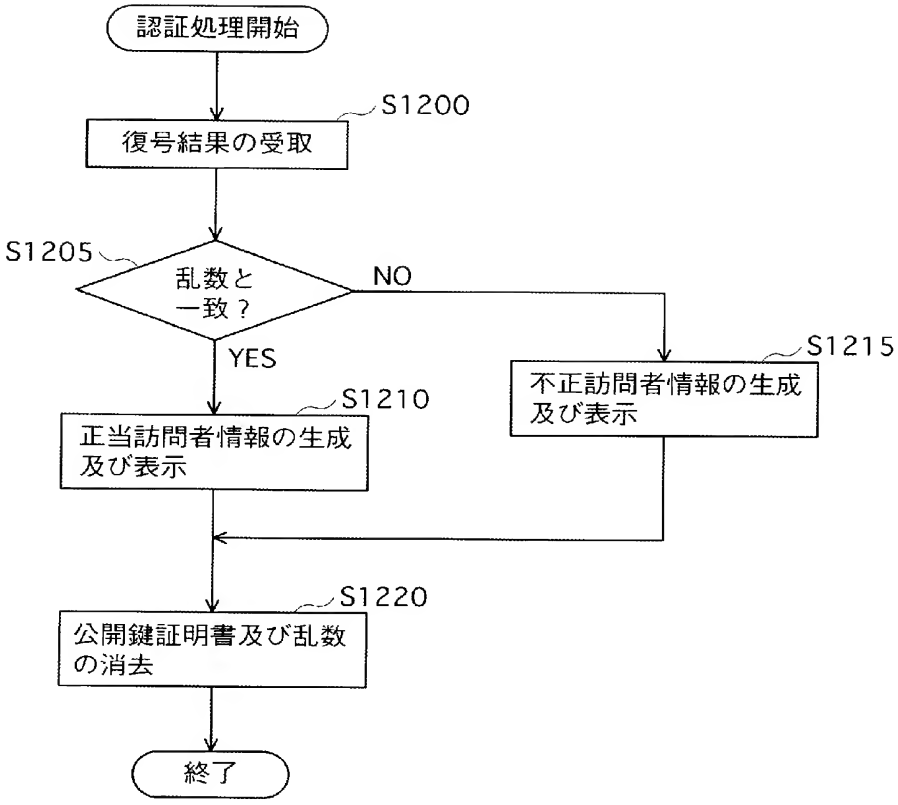
[図37]


ユーザ端末 1020
カードリーダ 1030
認証カード 1010
S1000
認証カードの挿入検知
S1005
検知情報及び証明書要求情報の生成
S1010
公開鍵証明書の取得
S1015
公開鍵証明書の受取
S1020
公開鍵証明書及び検知情報の出力
S1025
検証処理
S1030
乱数の生成
S1035
公開鍵の取得
S1040
暗号化情報の生成
S1045
暗号化情報の出力
S1050
暗号化情報の復号
S1055
復号結果の出力
S1060
認証処理

[図38]


検証処理開始
S1100
公開鍵証明書及び検知情報の受取
S1105
CA公開鍵の取得
S1110
公開鍵証明書の検証
S1115
検証OK？
NO
YES
S1125
不正訪問者情報の生成及び表示
S1120
公開鍵証明書の記憶
終了
S1030へ

[図39]


認証処理開始
S1200
復号結果の受取
S1205
乱数と
一致？
NO
YES
S1215
不正訪問者情報の生成
及び表示
S1210
正当訪問者情報の生成
及び表示
S1220
公開鍵証明書及び乱数
の消去
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017758

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2003-141664 A (Hitachi, Ltd.), 16 May, 2003 (16.05.03), Full text; all drawings (Family: none)	1-3,31-33, 39,40,46-48 4-30,34-38, 41-45
Y	JP 11-259712 A (Dainippon Printing Co., Ltd.), 24 September, 1999 (24.09.99), Full text; all drawings (Family: none)	4-30,34-38, 41-45
Y	JP 2001-243345 A (Oki Electric Industry Co., Ltd.), 07 September, 2001 (07.09.01), Full text; all drawings (Family: none)	8-15,35,36

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 January, 2005 (20.01.05)	08 February, 2005 (08.02.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017758

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Yoichi SHIBATA et al., Mechanism Base PKI, Computer Security Symposium 2003 Ronbunshu (Information Processing Society of Japan Symposium Series Vol.2003, No.15), 29 October, 2003 (29.10.03), pages 181 to 186	18,23

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１７７５８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ.Ｃｌ⁷　Ｇ０６Ｆ１７／６０

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ.Ｃｌ⁷．Ｇ０６Ｆ１７／６０

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国登録実用新案公報	１９９４－２００５年
日本国実用新案登録公報	１９９６－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ，ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ２００３－１４１６６４　Ａ（株式会社日立製作所） ２００３．０５．１６，全文，全図（ファミリーなし）	1-3, 31-33, 39, 40, 46-48
Ｙ		4-30, 34-38, 41-45
Ｙ	ＪＰ１１－２５９７１２　Ａ（大日本印刷株式会社） １９９９．０９．２４，全文，全図（ファミリーなし）	4-30, 34-38, 41-45
Ｙ	ＪＰ２００１－２４３３４５　Ａ（沖電気工業株式会社） ２００１．０９．０７，全文，全図（ファミリーなし）	8-15, 35, 36

☒　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２０．０１．２００５	国際調査報告の発送日 08. 2. 2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｌ　９４６７ 谷口　信行 電話番号　０３－３５８１－１１０１　内線　３５６０

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	柴田陽一　外，メカニズムベースＰＫＩ，コンピュータセキュリティシンポジウム２００３論文集（情報処理学会シンポジウムシリーズVol.2003, No.15），２００３．１０．２９，pp.181-186	18, 23